This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

Über dieses Buch

Dies ist ein digitales Exemplar eines Buches, das seit Generationen in den Regalen der Bibliotheken aufbewahrt wurde, bevor es von Google im Rahmen eines Projekts, mit dem die Bücher dieser Welt online verfügbar gemacht werden sollen, sorgfältig gescannt wurde.

Das Buch hat das Urheberrecht überdauert und kann nun öffentlich zugänglich gemacht werden. Ein öffentlich zugängliches Buch ist ein Buch, das niemals Urheberrechten unterlag oder bei dem die Schutzfrist des Urheberrechts abgelaufen ist. Ob ein Buch öffentlich zugänglich ist, kann von Land zu Land unterschiedlich sein. Öffentlich zugängliche Bücher sind unser Tor zur Vergangenheit und stellen ein geschichtliches, kulturelles und wissenschaftliches Vermögen dar, das häufig nur schwierig zu entdecken ist.

Gebrauchsspuren, Anmerkungen und andere Randbemerkungen, die im Originalband enthalten sind, finden sich auch in dieser Datei – eine Erinnerung an die lange Reise, die das Buch vom Verleger zu einer Bibliothek und weiter zu Ihnen hinter sich gebracht hat.

Nutzungsrichtlinien

Google ist stolz, mit Bibliotheken in partnerschaftlicher Zusammenarbeit öffentlich zugängliches Material zu digitalisieren und einer breiten Masse zugänglich zu machen. Öffentlich zugängliche Bücher gehören der Öffentlichkeit, und wir sind nur ihre Hüter. Nichtsdestotrotz ist diese Arbeit kostspielig. Um diese Ressource weiterhin zur Verfügung stellen zu können, haben wir Schritte unternommen, um den Missbrauch durch kommerzielle Parteien zu verhindern. Dazu gehören technische Einschränkungen für automatisierte Abfragen.

Wir bitten Sie um Einhaltung folgender Richtlinien:

+ *Nutzung der Dateien zu nichtkommerziellen Zwecken* Wir haben Google Buchsuche für Endanwender konzipiert und möchten, dass Sie diese Dateien nur für persönliche, nichtkommerzielle Zwecke verwenden.

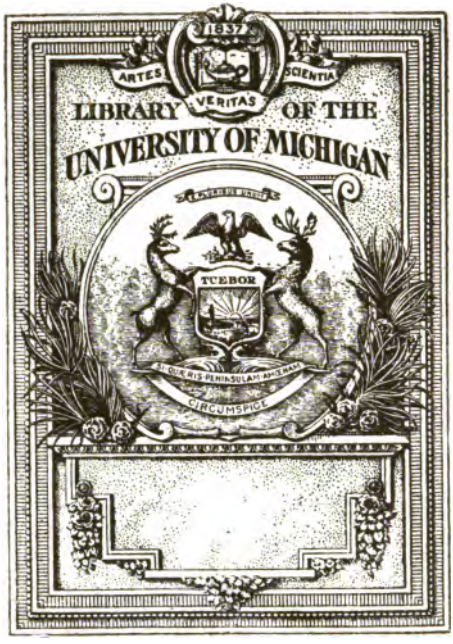
+ *Keine automatisierten Abfragen* Senden Sie keine automatisierten Abfragen irgendwelcher Art an das Google-System. Wenn Sie Recherchen über maschinelle Übersetzung, optische Zeichenerkennung oder andere Bereiche durchführen, in denen der Zugang zu Text in großen Mengen nützlich ist, wenden Sie sich bitte an uns. Wir fördern die Nutzung des öffentlich zugänglichen Materials für diese Zwecke und können Ihnen unter Umständen helfen.

+ *Beibehaltung von Google-Markenelementen* Das "Wasserzeichen" von Google, das Sie in jeder Datei finden, ist wichtig zur Information über dieses Projekt und hilft den Anwendern weiteres Material über Google Buchsuche zu finden. Bitte entfernen Sie das Wasserzeichen nicht.

+ *Bewegen Sie sich innerhalb der Legalität* Unabhängig von Ihrem Verwendungszweck müssen Sie sich Ihrer Verantwortung bewusst sein, sicherzustellen, dass Ihre Nutzung legal ist. Gehen Sie nicht davon aus, dass ein Buch, das nach unserem Dafürhalten für Nutzer in den USA öffentlich zugänglich ist, auch für Nutzer in anderen Ländern öffentlich zugänglich ist. Ob ein Buch noch dem Urheberrecht unterliegt, ist von Land zu Land verschieden. Wir können keine Beratung leisten, ob eine bestimmte Nutzung eines bestimmten Buches gesetzlich zulässig ist. Gehen Sie nicht davon aus, dass das Erscheinen eines Buchs in Google Buchsuche bedeutet, dass es in jeder Form und überall auf der Welt verwendet werden kann. Eine Urheberrechtsverletzung kann schwerwiegende Folgen haben.

Über Google Buchsuche

Das Ziel von Google besteht darin, die weltweiten Informationen zu organisieren und allgemein nutzbar und zugänglich zu machen. Google Buchsuche hilft Lesern dabei, die Bücher dieser Welt zu entdecken, und unterstützt Autoren und Verleger dabei, neue Zielgruppen zu erreichen. Den gesamten Buchtext können Sie im Internet unter `http://books.google.com` durchsuchen.



THE GIFT OF
PROF. ALEXANDER ZIWET

Mathematics
QA
245
.S32

494

Alexander Ziwet

BEITRÄGE

ZUR

ZAHLENTHEORIE,

INSBESONDERE ZUR

KREIS- UND KUGELTHEILUNG

MIT EINEM NACHTRAGE ZUR

THEORIE DER GLEICHUNGEN.

VON

DR. HERMANN SCHEFFLER.

LEIPZIG.
VERLAG VON FRIEDRICH FOERSTER.
1891.

Prof. A. Zimet
qt
12-21-1922

Math

Inhalt.

Seite

Einleitung V

I. Die konstruirbare Kreistheilung.

§. 1. Die Zurückführung der binomischen Gleichung höheren Grades auf Gleichungen niedrigerer Grade 1
§. 2. Auflösung der Gleichung $x^p - 1 = 0$ 26
§. 3. Konstruktion des Polygons von p Seiten 27

II. Die zyklisch geordneten Funktionen.

§. 4. Die zyklisch geordneten Funktionen 35

III. Die allgemeine Kreistheilung.

§. 5. Die Periodengleichungen für beliebige Primzahlen 49
§. 6. Independente Formeln 68
§. 7. Die vollständige Auflösung 106
§. 8. Die geometrische Bedeutung der Perioden 120
§. 9. Die Fälle, wo p keine Primzahl ist 123
§. 10. Zurückführung der Periodengleichungen auf Gleichungen mit reellen Koeffizienten und Wurzeln 132
§. 11. Aufsuchung der primitiven Wurzeln 133
§. 12. Die geometrische Konstruktion der Gleichungen und namentlich der regelmässigen Polygone 143

IV. Die Theilbarkeit der Zahlen von der Form $2^r + 1$.

§. 13. Zerlegung dieser Zahlen 147
§. 14. Kennzeichnung der Theilbarkeit durch die Kongruenzen 173
§. 15. Die Reste der Potenzen eines Binoms 178
§. 16. Die Anzahl und Höhe der Primzahlen 182

V. Zur allgemeinen Zahlentheorie.

§. 17. Die polyplexen Wurzeln einer Gleichung und die polyplexe Zahl überhaupt 195
§. 18. Die ideale Zahl 217
§. 19. Die algebraische Zahl 225
§. 20. Die Quaternion 232

VI. Die Kugeltheilung.

§. 21. Die regelmässige Eintheilung der Kugeloberfläche 237

Anhang.

VII. Zur Theorie der Gleichungen.

§. 22. Das Lösbarkeitsmerkmal und die Herstellung lösbarer Gleichungen 246

9-21-32 MEW

413321

Einleitung.

Gauss hat im siebenten Abschnitte der an neuen Ideen so reichen Disquisitiones arithmeticae die Kreistheilung begründet, den weiteren Ausbau dieser Theorie jedoch der Nachwelt überlassen. Nachdem derselbe nachgewiesen hatte, dass ein regelmässiges Vieleck geometrisch konstruirbar, also die Theilung des Kreises auf quadratische Gleichungen zurückführbar sei, wenn die Seitenzahl eine Primzahl von der Form $2^r + 1$ ist, und nachdem er in Art. 365 die spezielle Auflösung für das Siebzehneck gegeben hatte, ist die Auflösung des nächstfolgenden Falles, nämlich der Theilung des Kreises in $2^8 + 1 = 257$ Theile von Richelot im 9-ten Bande von Crelle's Journal für Mathematik mittelst einer Rechnung vollzogen, welche elf Bogen in Anspruch nimmt, sich also als ein sehr umständliches Verfahren erweis't. Auch die Darstellung in Serret's algèbre supérieure, 28me leçon, welche wörtlich in Schnuse's Theorie der Kreisfunktionen S. 112 bis 122 (selbst mit einem Druckfehler in dem Ausdrucke für $y\,y_1$) übergegangen ist, lässt eine bestimmte Regel vermissen, nach welcher die Koeffizienten der Gleichungen, von denen die Lösung der Aufgabe abhängt, aus den schon von Gauss angegebenen Eigenschaften dieser Koeffizienten zu bestimmen sind.

Kummer hat in der Abhandlung über die Zerlegung der Wurzeln der Einheit im 35-sten Bande von Crelle's Journale die Regeln zur Aufstellung der Periodengleichungen nicht nur für die konstruirbaren, sondern auch für die übrigen Fälle verallgemeinert, und Bachmann hat, gestützt auf diese Regeln, in seiner Lehre von der Kreistheilung die Theorie nach ihrem heutigen Standpunkte sehr übersichtlich dargestellt. Trotz dieser Fortschritte ist der Gegenstand noch nicht abgeschlossen, und selbst innerhalb des Rahmens, welchen die Theorie heute einnimmt, sind verschiedene Mängel zu verzeichnen.

Zunächst bedürfen die von Kummer entdeckten Eigenschaften der Koeffizienten der linearen Ausdrücke für die Produkte zweier Perioden einer weiteren Bearbeitung zu einer allgemeinen Regel, nach welcher die Tafel dieser Koeffizienten, wenn $p = r\,s + 1$ ist, für jeden beliebigen Werth von r in ihrer allgemeinsten Form aus der geringsten Zahl wirklich unbekannter Grössen herzustellen ist. Ausserdem ist die in dieser Koeffiziententafel nothwendig erscheinende Anzahl von unbekannten Grössen bis jetzt nicht bestimmt, ein Mangel, welcher über die Zulänglichkeit der schliesslich aufzustellenden Gleichungen und über die daraus abzuleitende Form der Primzahl p die grösste Ungewissheit bestehen lässt.

Sodann fehlt es noch an der allgemeinen Regel, durch welche die symmetrischen Funktionen mit beliebig viel Dimensionen in den linearen Perioden sicher herzustellen sind, was eine Zerlegung in zyklisch geordnete Bestandtheile für jeden beliebigen Werth von r und s voraussetzt. Diese beiden Unvollkommenheiten werden auch wohl Bachmann veranlasst haben, seine Untersuchungen auf die Anfangsfälle $r = 2, 3, 4$ zu beschränken, ohne für den allgemeinen Fall den Weg vorzuzeichnen.

Die erwähnten beiden Mängel erachte ich indess für klein gegen den dritten, welcher darin besteht, dass die Gleichung $x^p - 1 = 0$ durch die bisherige Theorie gar nicht aufgelös't werden kann. Zur Begründung dieser Behauptung mache ich darauf aufmerksam, dass, wenn $p = (r\, r'\, r'' \ldots) + 1$ gesetzt wird, zuerst eine Gleichung r-ten Grades zu lösen ist, welche r Wurzeln hat. Diese r Wurzeln treten sodann in ein System von r Gleichungen r'-ten Grades ein, um deren Koeffizienten zu bestimmen: zur Aufstellung dieses Systems ist aber die Kenntniss des Werthes der gedachten r Wurzeln nicht ausreichend, diese Wurzeln müssen vielmehr nach einer gewissen gesetzlichen Reihenfolge in die letzteren Koeffizienten eingesetzt werden; ohne Kenntniss dieses Gesetzes ist das fragliche System von Gleichungen nicht aufzustellen und nicht zu lösen, es sind also schon für das nächstfolgende System noch nicht einmal die Werthe der Wurzeln, geschweige deren Reihenfolge darzustellen, mithin ist die Aufgabe nicht zu Ende zu führen. Bachmann ist dieser Mangel nicht entgangen; er hebt ihn in seiner Kreistheilung auf S. 217 hervor, indem er sagt, dass „die Bestimmung der Perioden für $r = 3$ erst dann möglich sei, wenn die Frage gelös't ist, welche der drei Kubikwurzeln für T_1 und T_2 zu wählen sei, eine Frage, welche ihrer Lösung noch harret". Demzufolge brechen auch alle Untersuchungen über die Kreistheilung mit der die erste Zerlegung darstellenden Gleichung ab und beschränken sich auf Betrachtungen über diese erste Gleichung.

Nur ein einziger Fall ist ohne Kenntniss der fraglichen Reihenfolge zu erledigen, nämlich der, wo $p - 1$ nur den Primfaktor 2 enthält, also $= 2^r$ ist, weil es sich hierbei nur um quadratische Gleichungen handelt, für welche die Reihenfolge der beiden Wurzeln gleichgültig ist. Da dieser Fall von hervorragender Wichtigkeit ist und nicht des Beistandes spezieller Hülfstheorieen bedarf, jedoch bis jetzt eines generellen und doch einfachen Auflösungsverfahrens entbehrt; so habe ich denselben in §. 1 bis 3 nach einer selbstständigen Regel für sich behandelt.

In §. 3 habe ich eine einfache geometrische Konstruktion mitgetheilt, welche auf jedes konstruirbare Vieleck anwendbar ist und alle p Seiten auf einmal oder das vollständige Vieleck ergiebt, wie aus der ausgeführten Konstruktion des Siebzehneckes ersichtlich ist. Die von Serret angegebene und von Schnuse wiederholte Konstruktion geht nicht über das Siebzehneck hinaus und ergiebt nur eine einzige Seite. Die von Staudt in Crelle's Journal Bd. 24 ohne Beweis mitgetheilte und von Bachmann wiedergegebene, nach Schröter etwas modifizirte Konstruktion liefert zwar alle Eckpunkte des Siebzehneckes, ist jedoch ziemlich verwickelt, bedarf eines umfangreichen Beweises und ist doch so, wie sie eben liegt, nur für das Siebzehneck anwendbar.

Hiernächst erschien es mir nöthig, in §. 4 eine Untersuchung über die zyklisch geordneten Funktionen anzustellen und dadurch den sicheren Grund zur Darstellung der höheren symmetrischen Funktionen und zur Beseitigung des zweiten vorhin erwähnten Mangels zu legen.

Sodann habe ich in §. 5 bis 12 die allgemeinen Periodengleichungen behandelt. Ich bin dabei meinem eigenen Wege gefolgt und habe zuerst in §. 5 die Aufstellung dieser Gleichungen durch rekursorisches Verfahren, welches Hülfstheorien ganz entbehrlich macht, gezeigt. Darauf habe ich in §. 6 independente Formeln folgen lassen, welche mich zu den schon von Kummer gefundenen Beziehungen zwischen den Koeffizienten der linearen Ausdrücke der Produkte der Perioden leiteten, in weiterer Behandlung aber die bis jetzt noch unbekannte bestimmte Regel zur Aufstellung der Koeffiziententafel aus der kleinstmöglichen Zahl unbekannter Elemente herbeiführten. Ausserdem ist daselbst in Nr. 6 die Anzahl der unbekannten Koeffizienten bestimmt ermittelt, deren genaue Kenntniss über die Zulänglichkeit der schliesslich aufzustellenden Gleichungen und die Form der Primzahl p von grösster Bedeutung ist.

In Nr. 24 des §. 6 ist sodann der Weg, welcher zu der quadratischen, kubischen oder höheren Form der Primzahl p oder einer ganzzahligen Funktion dieser Zahl führt, bestimmt vorgezeichnet.

Endlich ist in §. 7 die vollständige Auflösung der Gleichung $x^p - 1 = 0$ gelehrt, indem daselbst das Gesetz der Reihenfolge der Wurzeln der verschiedenen Periodengleichungen ermittelt worden ist.

In §. 9 ist die Theorie der Kreistheilung auf die Fälle, wo p eine zusammengesetzte Zahl ist, erweitert.

Da die Auflösung der Periodengleichungen neben reellen auch komplexe Wurzeln ergiebt; so würde man auf die Entstehung von Gleichungen mit komplexen Koeffizienten gefasst sein müssen. In §. 10 ist gezeigt, wie Dem zu entgehen ist.

Da man zur Aufstellung einer Grundtafel nothwendig eine primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \ mod\ p$ kennen muss; so habe ich in §. 11 eine Anzahl von Sätzen mitgetheilt, welche diese Auffindung erleichtern.

Die Kreistheilung hat vornehmlich durch die Konstruirbarkeit des regelmässigen Vieleckes von p Seiten, wofür $p - 1 = 2^r$ nur den Primfaktor 2 hat, insbesondere des Siebzehneckes, ihre Berühmtheit erlangt. Demzufolge wird der in §. 12 geführte Nachweis, dass jedes regelmässige Vieleck, dessen Seitenzahl eine Primzahl p ist, wenn $p - 1 = 2^r 3^s$ nur die Primfaktoren 2 und 3 hat, durch Kegelschnitte konstruirbar ist, und dass das Nämliche auch geschehen kann, wenn die Seitenzahl p keine Primzahl ist, aber die Form $2^r 3^s$ hat, einiges Interesse in Anspruch nehmen. Mit Kegelschnitten, welche mittelst geeigneter Instrumente ebenso gut in stetigen Zügen beschrieben werden können, wie der Kreis und die gerade Linie mit Zirkel und Lineal zu beschreiben sind, kann also z. B. das Siebeneck, das Neuneck, das Dreizehneck, das Neunzehneck konstruirt werden. Die einfache Konstruktion des Siebeneckes ist in §. 12 Nr. 4 ausgeführt.

Nachdem die Ansicht Legendre's, dass jede Zahl von der Form $2^r + 1$, worin r eine Potenz von 2 ist, eine Primzahl sei, durch Euler's Wahrnehmung, dass die Zahl $2^{32} + 1 = 4\ 294\ 967\ 297$ den Faktor 641 habe, widerlegt war, blieb es, wie auch Bachmann in seinem Buche auf S. 68 anmerkt, zweifelhaft, ob der Kreis auf unendlich viel verschiedene Weise mit Zirkel und Lineal getheilt werden kann. Ob Euler durch Probedivisionen, für welche die Kleinheit des Faktors 641 ein günstiger Zufall war, zu jener Wahrnehmung gelangte, ist mir nicht bekannt. Da nun das einzige sichere Merkmal einer Primzahl, der Wilsonsche Lehrsatz, bei so grossen Zahlen wegen des ungeheueren Zahlenaufwandes, den er erfordert, seine Dienste versagt; so habe ich mich um die Auffindung leichter anwendbarer Mittel zur Erkenntniss der Theilbarkeit einer Zahl von der Form $2^r + 1$ bemüht und die Ergebnisse in §. 13 und 14 mitgetheilt. Namentlich enthält §. 14 ein neues und leicht zu konstatirendes Merkmal für Primzahlen, welche eine gewisse Form haben. Die in §. 15 mitgetheilte Formel für den Rest der Potenz eines Binoms wird unter Umständen bei zahlentheoretischen Untersuchungen nützliche Dienste leisten können.

In §. 16 findet sich ein kurzer Beweis über die Unendlichkeit der Primzahlen und ein Verfahren zur Bestimmung der zwischen gegebenen Grenzen liegenden und überhaupt aller Primzahlen. Auch habe ich darin eine allgemeine Formel für eine Primzahl angegeben.

Kreistheilung ist doch nur der Titel für einen gewissen Abschnitt der Zahlentheorie, d. h. der Lehre von den ganzen Zahlen: der Kern derselben liegt in den Gesetzen gewisser Primzahlen, welche aus dem Zusammenhange zwischen Kongruenzen und Gleichungen höherer Grade gewonnen werden und wegen der geometrischen Bedeutung jedes algebraischen Polynoms die geometrischen Gesetze der Polygone zur Erkenntniss bringen. Der Begriff der ganzen Zahl ist übrigens von seiner ursprünglichen Bedeutung als Vielfaches der Einheit allmählich zu dem Begriffe der ganzen rationalen Funktion erweitert und hat auf diese Weise eine allgemeine Zahlentheorie ins Leben gerufen. Während einerseits die Zerlegbarkeit als eine, wennauch in ihrer Bedeutung erweiterte Grundvorstellung festgehalten wurde, verfolgte die Verallgemeinerung unverkennbar das Ziel, die den elementaren Gesetzen der ganzen reellen und komplexen Zahlen entsprechenden Beziehungen im allgemeinen Zahlengebiete als Beziehungen zwischen entsprechenden allgemeineren Grössenbildungen darzulegen. Diese Arbeiten legen Zeugniss für den mächtigen Schwung des mathematischen Geistes ab; allein, sie sind zum Theil Missdeutungen fähig, welche daraus entspringen, dass die wahren, allgemeinen und unerschütterlichen Grundlagen der Mathematik heute noch nicht als solche erkannt oder anerkannt sind, sodass es erlaubt erscheint, jede Hypothese zur Grundlage einer mathematischen Theorie, jeden Vorgang zu einer Grundoperation, jede Vorstellung für eine mathematische Wirklichkeit, jede Idee für eine Grösse zu nehmen. Hieraus entspringt der allgemeine Irrthum, dass die in der allgemeinen Zahlentheorie geschaffenen Funktionen die Vertreter aller möglichen Grössen im allgemeinen Zahlengebiete seien, ein Irrthum, der darin wurzelt, das das Wesen einer wahren Dimension oder eines echten Qualitätsgrades nicht gewürdigt, sondern mit der

Variabilität nach jeder beliebigen Koordinatenaxe oder Mannichfaltigkeitsrichtung desselben Partialgebietes, in welchem die Operationen vorgenommen werden, verwechselt wird. Die Resultate aller bisherigen Zahlentheorien haben nur eine Bedeutung für die Grössen der komplexen Zahlenebene, nicht für den Zahlenraum und das noch allgemeinere Zahlengebiet. Es ist undenkbar, dass das grösste mathematische Genie mit den Mitteln, welche die übergrosse Mehrheit der Mathematiker heute noch als die zulässigen und ausreichenden anerkennt, über die Zahlenebene hinauszuschreiten vermöchte. Diese Fessel ist ein absoluter Zwang, welcher das Aufsteigen durchaus unmöglich macht und daher einen Jeden, welcher sich der Täuschung hingiebt, mit jenen Mitteln die Schranke durchbrochen zu haben und in das allgemeine Zahlengebiet eingedrungen zu sein, zu einer Reihe von falschen Schlüssen nöthigt, welche den unbefangenen Denker bald mehr, bald weniger betroffen machen und das fast unglaubliche Schauspiel darbieten, dass die neuere Mathematik sich mit Kontroversen füllt.

Dieser Zusammenhang und diese Erwägung hat mich zu den §§. 17 bis 21 über die allgemeine Zahlentheorie veranlasst. In §. 17 habe ich die polyplexe oder die natürliche Zahl, als den auf die Grundeigenschaften der Grössen gestützten Begriff der allgemeinen Zahl des gesammten Grössengebietes vorgeführt und dabei verschiedene der in neuerer Zeit entstandenen Irrthümer aufgedeckt.

In §. 18 habe ich die ideale Zahl, in §. 19 die algbraische Zahl und in §. 20 die Quaternion einer kritischen Beleuchtung unterzogen.

Der §. 21 schliesst die Schrift mit einer Erweiterung der Kreistheilungslehre auf die Kugeltheilung und zeigt zugleich eine interessante Anwendung meines Situationskalkuls auf die Bestimmung der regelmässigen Polyeder.

Der Anhang enthält in §. 22 eine weitere Erörterung über das allgemeine Merkmal der Lösbarkeit der Gleichungen, welches ich in den kürzlich erschienenen „Beiträgen zur Theorie der Gleichungen“ aufgestellt habe.

In Beziehung auf diese Schrift mache ich noch die Bemerkung, dass mir bei Abfassung derselben von Serret's Cours d'algèbre supérieure die erste Ausgabe vom Jahre 1849 vorgelegen hat. Aus der mir soeben zu Gesicht gekommenen vierten Ausgabe ersehe ich, dass im 2-ten Bande vom Jahre 1879 nachträglich die Arbeiten von Galois berücksichtigt sind, von welchen ich auf S. 57 meiner Schrift gesagt habe, dass sie fehlen. Was übrigens die von mir behauptete Unzulänglichkeit der bisherigen Theorie betrifft; so ist dieselbe auch in der vierten Ausgabe noch vorhanden: der von mir auf S. 62 meiner Schrift zitirte, mit den Worten „Tel est le point“ beginnende Satz findet sich jetzt auf S. 496 des gedachten zweiten Bandes.

Dieser Band enthält im Kapitel V einige Untersuchungen über die Höhe der Primzahlen, welche jedoch mit den meinigen in §. 16 der gegenwärtigen Schrift angestellten nicht in Konkurrenz treten.

Da ich von dem Werke der Herren E. und U. Dühring „Neue Grundmittel und Erfindungen zur Analysis u. s. w.“ vom Jahre 1884,

welches unter Anderem auch die Theorie der Gleichungen behandelt, erst nach der Veröffentlichung der vorerwähnten Schrift Kenntniss erlangt habe; so bleibt mir nur übrig, meine Ansicht darüber in dem Anhange der gegenwärtigen Schrift auszusprechen. Ich habe dort meine Bemerkungen auf die „Werthigkeitsrechnung" beschränkt, welche ich für sehr anfechtbar und für die Auflösung der Gleichungen nicht für zulänglich halte. Was die übrigen in dem Dühringschen Werke ausgesprochenen Ansichten über gewisse Grundlagen der Mathematik, z. B. über die Bedeutung des Negativen und des Imaginären betrifft; so hat mich die Zuversicht, womit schwere Irrthümer für Wahrheiten ausgegeben werden, sowie die Dreistigkeit, womit die tiefsten Denker wie Gauss, Jacobi, Dirichlet auf S. 29, 30, 59 und an anderen Orten für unbedeutende Geister und irrende Phantasten erklärt werden, in das höchste Erstaunen versetzt, welchem ich mich gedrungen fühle, hier Ausdruck zu geben. Zur Begründung dieses Urtheils wird es genügen, anzuführen, dass die Verfasser auf S. 30 ihres Werkes die Gausssche Deutung der imaginären Grösse $\sqrt{-1}$ mit der Erklärung zu persifliren suchen, dass es „hochkomisch sei, eine negative Abszisse mit einer positiven multipliziren zu wollen, da schon der blühendste Unsinn zu haben sei, wenn man sie zu einander auch nur addire: nach dieser Logik müsse nämlich die Länge zwischen dem Endpunkte der negativen und demjenigen einer gleichen positiven Abszisse ganz unverdrossen null sein". Wenn die Verfasser aus der Additionsformel $(+x) + (-x) = 0$ den Schluss ziehen, dass der Abstand der Endpunkte von $+x$ und $-x$ gleich null sei, oder dass diese Endpunkte zusammenfallen; so bekunden sie damit, dass ihnen der wahre Sinn der Addition noch verschlossen geblieben ist. Die Addition, als zweite Grundoperation, ist nicht mit der ersten Grundoperation, nämlich mit der Numeration oder Zusammenzählung identisch; sie bedeutet vielmehr Aneinanderreihung. Während die Numerationsformel $a + b$, worin das Zeichen $+$ als Summationszeichen gebraucht wird, die Zusammenzählung der in a und b enthaltenen Einheiten verlangt, fordert die Additionsformel $a + b$, worin das Zeichen $+$ als Anreihungs- oder Angliederungssymbol gebraucht wird, dass der Anfangspunkt des zweiten Gliedes b an den Endpunkt des ersten Gliedes gelegt werde, wodurch sehr deutlich $(+x) + (-x) = 0$ wird. Der Schluss, dass der Abstand der beiden Endpunkte von $+x$ und $-x$ gleich null sei, fusst auf der falschen Vorstellung, dass bei der Addition von $-x$ zu $+x$ der Anfangspunkt des zweiten Gliedes b an den Anfangspunkt des ersten Gliedes a gelegt werde. Wer diesen falschen Schluss macht, beweis't, dass ihm das wahre Wesen der mathematischen Grundeigenschaften und Grundoperationen, insbesondere die richtige Erkenntniss des Wesens des Negativen und des Imaginären noch verborgen ist, und dass ihm weder das Recht zusteht, über Männer wie Gauss zu spötteln, „nebelhafte Wüstheit für den maassgebenden Charakterzug des gesammten jetzigen mathematischen Treibens" (S. 399) zu erklären, noch für seine neuen Grundlagen Anerkennung zu beanspruchen.

Ebenso thöricht ist die auf S. 29 und 30 beliebte Verhöhnung der Ansicht, dass $\sqrt{-1}$ die mittlere geometrische Proportionale zwischen

$+1$ und -1 sei, und dass diese Grösse die geometrische Bedeutung der auf der reellen Axe normal stehenden Längeneinheit habe. Diese Ansicht, welche für einen Aberglauben erklärt wird, „den auch dieser Gauss erbte, dem er wahlverwandt war", beruht auf einer sehr richtigen Auffassung und begründet sich damit, dass (wie ich in §. 22 Nr. 11 etwas näher ausgeführt habe) die Zeichen $+$, $-$, $\sqrt{-}$ oder i durchaus nicht bloss Operationszeichen sind, sondern auch dazu dienen, die dritte Grundeigenschaft der Grössen, nämlich ihre Relation oder ihr Verhältniss zur Grundeinheit darzustellen, was den Spöttern noch nicht zur Erkenntniss gekommen ist und ihre Pfeile auf sie selber zurück lenkt.

Allerdings haben sich die grossen Mathematiker bisher nur mit der Erweiterung spezieller Gebiete der Wissenschaft, nicht mit der Ermittlung der Grundlagen derselben befasst, vielmehr die hierüber herrschenden Irrthümer und Unklarheiten fortbestehen lassen: allein durch das Dühringsche Werk hat sich die Zahl derselben nur vermehrt, und an die Stelle der Klärung der Begriffe ist eine neue Verwirrung getreten. Möglicherweise fällen die Verfasser jenes Werkes über die Ansichten, welche ich über die fraglichen Grundlagen in den unter dem Titel „die Naturgesetze", „die Welt nach menschlicher Auffassung" und „die Grundlagen der Wissenschaft" erschienenen Schriften niedergelegt habe, ein ähnliches Urtheil, wie ich über die ihrigen, und würden, wenn sie es thäten, hiermit nicht allein stehen, da diese Ansichten auch sonst noch kein Verständniss gefunden haben: ich würde daher ein abfälliges Urtheil auch von jener Seite mit derselben Ruhe ertragen, mit welcher ich meine Ansichten über die Grundprinzipien der Welt im Strome der herrschenden Anschauungen unter dem gewaltigen Drucke der Schule versinken sehe, hoffend, dass doch einmal der Tag kommen werde, wo sie wieder auftauchen und an einem sicheren Orte im Reiche der rationellen Geistesarbeit geborgen werden.

I. Die konstruirbare Kreistheilung.

§. 1. Die Zurückführung der binomischen Gleichung höheren Grades auf Gleichungen niedrigerer Grade.

1) Die binomische Gleichung $x^p - 1 = 0$, welche algebraisch in der Form $x = \sqrt[n]{1}$ lösbar ist, würde vom Standpunkte der algebraischen Auflösung der Gleichungen, d. h. zum Zweck der Darstellung ihrer Wurzeln durch Wurzelausdrücke keiner weiteren Behandlung bedürfen. Das Interesse, welches sich an diese Behandlung knüpft, betrifft daher nicht die Erkenntniss des Werthes jener Wurzeln, sondern die Form, in welcher sich dieselben darstellen lassen, und insbesondere die Zahlengesetze, welche sich dabei enthüllen und welche in ihren Hauptzügen zuerst von Gauss dargelegt sind.

Wenn die vorstehende Gleichung durch Division mit $x - 1$ von der Wurzel $x = 1$ befreiet wird, hat die Gleichung $(p-1)$-ten Grades

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

die $p - 1$ Wurzeln $\alpha, \alpha^2, \alpha^3 \ldots \alpha^{p-1}$, worin $\alpha = e^{\frac{2\pi i}{p}}$ den Fundamentalwerth der Einheitswurzel vom Grade p bedeutet. Nehmen wir von jetzt an für p eine unpaare Primzahl; so sind alle Wurzeln dieser Gleichung komplex und verschieden. Statt der vorstehenden Gleichung

$$(1) \qquad x^1 + x^2 + x^3 + \ldots + x^{p-1} = -1$$

kann man auch, indem man zur Abkürzung $\frac{p-1}{2} = m$ setzt, die durch Division mit x^m sich ergebende Gleichung

$$(2) \qquad X_1 + X_2 + X_3 + \ldots + X_m = -1$$

worin $(3) \quad X_r = x^r + x^{-r}$

ist, sodass man die allgemeinen Beziehungen

$$(4) \qquad X_{-r} = X_r \quad \text{und} \quad X_r \,.\, X_s = X_{r+s} + X_{r-s}$$

hat. Das Ziel der Behandlung der Gleichung (1) oder (2) besteht nun darin, die Gesammtheit Y der Glieder dieser Gleichung so in Gruppen $Y_1, Y_2, \ldots Y_n$ zu ordnen, dass die symmetrischen Grundfunktionen dieser Gruppen, also die Werthe von $Y_1 + Y_2 + Y_3 +$ etc. $= A_1$,

$Y_1 Y_2 + Y_2 Y_3 + \text{etc.} = A_2$, $Y_1 Y_2 Y_3 + Y_2 Y_3 Y_4 + \text{etc.} = A_3$ u. s. w. aus dem Werthe -1 der Gesammtheit Y bestimmt werden kann, sodass der Werth der einzelnen Gruppen $Y_1, Y_2, \ldots Y_n$ durch Auflösung der Gleichung $x^n - A_1 x^{n-1} + A_2 x^{n-2} - \text{etc.} = 0$ erfolgen kann. Wenn sich hierbei zeigt, dass sich jede Gruppe auf ähnliche Weise wiederum in niedrigere Gruppen ordnen lässt, deren symmetrische Funktionen in ähnlicher Weise aus den höheren Gruppen bestimmbar sind; so wird die Berechnung der Grössen x oder X auf die Auflösung von Gleichungen niedrigerer Grade zurückgeführt und die Herstellung der Koeffizienten dieser Gleichungen, da hierzu ausser den Koeffizienten der Gleichung (1) oder (2), welche sämmtlich $= 1$ sind, weiter keine Grösse, als die Primzahl p gegeben ist, bringt gewisse Zahlengesetze, welche die Eigenart der Primzahl p kennzeichnen, zum Vorschein.

Wenn a eine primitive Wurzel der Kongruenz $x^{p-1} - 1 \equiv 0 \; mod\; p$ ist, wenn also die $(p-1)$-te Potenz von a die niedrigste ist, welche den kleinsten Rest 1 liefert; so befinden sich unter den kleinsten positiven Resten der Potenzen

$$a^1 \; a^2 \; \ldots \; a^{p-2} \; a^{p-1}$$

oder

$$a^0 \; a^1 \; a^2 \; \ldots \; a^{p-2}$$

sämmtliche $p-1$ Zahlen 1, 2, 3 ... $(p-1)$ oder auch, wenn man statt der kleinsten positiven die absolut kleinsten Reste betrachten will, sämmtliche $\frac{p-1}{2}$ Zahlen 1, 2, 3 ... $\frac{p-1}{2}$ einmal mit positivem und einmal mit negativem Zeichen. Wenn es auf die Reihenfolge nicht ankömmt, kann man also für die Exponenten der Gleichung (1) oder für die Zahlen 1, 2, 3 ... $(p-1)$ die kleinsten positiven Reste der Potenzen $a^0, a^1, a^2 \ldots a^{p-1}$ setzen oder, wenn man diese Reste resp. mit $\varrho_1, \varrho_2 \ldots \varrho_{p-1}$ bezeichnet, kann man für jene Gleichung

$$(5) \qquad x^{\varrho_1} + x^{\varrho_2} + x^{\varrho_3} + \ldots + x^{\varrho_{p-1}} = -1$$

setzen. In der Gleichung (2) aber kann man für die Zeiger 1, 2, 3 ... m die verschiedenen absolut kleinsten Reste der Potenzen $a^0, a^1, a^2 \ldots a^{p-1}$, insofern dieselben nicht nach ihrem Zeichen unterschieden werden, nehmen oder, wenn man diese Reste mit $\varrho_1, \varrho_2 \ldots \varrho_m$ bezeichnet, kann man für jene Gleichung

$$(6) \qquad X_{\varrho_1} + X_{\varrho_2} + X_{\varrho_3} + \ldots + X_{\varrho_m} = -1$$

substituiren.

Die symmetrischen Funktionen von zwei und mehr Dimensionen der Gruppen $Y_1, Y_2 \ldots$ bilden sich aus diesen Gruppen durch Multiplikation der einzelnen Gruppen und diese Multiplikationen laufen, da jede Gruppe ein Inbegriff von Potenzen derselben Grundgrösse x ist, auf Additionen der Exponenten der Glieder jeder Gruppe hinaus. Behandelt man also die Gleichung (1) oder (5); so sind die zu addirenden Exponenten die kleinsten positiven Reste $\varrho_1, \varrho_2 \ldots \varrho_{p-1}$. Behandelt man aber die Gleichung (2) oder (6), deren Grad nur halb so hoch ist, als der der Gleichung (1); so sind behuf Darstellung irgend eines Produktes zweier Gruppen wie Y_1, Y_2 aus den Zeigern oder aus den absolut kleinsten

Resten $\varrho_1, \varrho_2 \ldots \varrho_m$ der Grössen X wegen der Beziehungen (4) sowohl die Summen, als auch die Differenzen zu bilden.

Die wesentliche Operation besteht hiernach in der Gruppirung der Reste so, dass sich aus den Resten, welche den einzelnen Gruppen angehören, durch Addition (resp. durch Addition und Subtraktion) die höheren Gruppen darstellen lassen, was dann, wenn es gelingt, die Erkenntniss mit sich führt, dass sich aus den einfachen Gruppen der Glieder der Gleichung (1) oder (2) die höheren Gruppen durch einen ganzzahligen rationalen Prozess darstellen lassen.

Übrigens schalten wir die Bemerkung ein, dass wenn man die Exponenten von x oder die Zeiger von X nach irgend einer Regel so ordnen kann, dass sie das vorstehende Resultat ergeben, es ganz gleichgültig ist, ob sie als die Reste der Potenzen einer Grösse a dargestellt sind oder nicht, dass sie aber thatsächlich immer solche Reste vertreten werden. In allen Fällen sind zwei Potenzen von x, deren Exponenten einander nach dem Model p kongruent sind, einander gleich, da $x^p = a^{np} = a^0 = 1$, also $x^{p+q} = x^q$ ist. Das Nämliche gilt von den Grössen X, da $X_p = x^p + x^{-p} = a^{np} + a^{-np} = 2$, also $X_{p \pm q} = X_q = X_{-q}$ ist.

2) Der Fall, wo der Grad p der ursprünglichen Gleichung eine Primzahl von der Form $2^r + 1$ oder $\frac{p-1}{2} = m = 2^{r-1}$ ist, zeichnet sich vor allen übrigen in so hohem Maasse aus, dass wir demselben eine dem allgemeineren Falle vorausgehende Behandlung in der Absicht widmen, zu zeigen, mit welchen einfachen Mitteln derselbe sich lösen lässt.

Dass $2^r + 1$ nur dann eine Primzahl sein kann, wenn r eine Potenz von 2 ist, auch dass nicht jede Zahl, welche diese Bedingung erfüllt, z. B. nicht die Zahl

$$2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$$

sondern nur manche dieser Zahlen, wie

$$2^1 + 1 = 3,\ 2^2 + 1 = 5,\ 2^4 + 1 = 17,\ 2^8 + 1 = 257,\ 2^{16} + 1 = 65537$$

eine Primzahl ist, bildet einen bekannten Satz.

Wir behandeln den Fall nach Gl. (6), stellen also zunächst als Grundtafel die Tafel der absolut kleinsten Reste $\varrho_1, \varrho_2 \ldots \varrho_m$ ohne Rücksicht auf das Zeichen derselben auf. Zu dem Ende setzen wir in die erste Horizontalreihe der Tafel die r Zahlen $2^0, 2^1, 2^2 \ldots 2^{r-1}$ oder 1, 2, 4 ... m, ohne zunächst danach zu fragen, von welchen Potenzen einer Zahl a Diess die Reste sind. Wir bemerken nur, dass der absolut kleinste Rest von 2^r wiederum 1 ist (da $2^r = p - 1 \equiv -1 \ mod\ p$) und dass keine niedrigere Potenz von 2 den Rest 1 haben kann.

Ist nun a eine primitive Wurzel der Kongruenz $x^{p-1} - 1 \equiv 0 \ mod\ p$, also a^{2m} die niedrigste Potenz von a, welche den kleinsten positiven Rest 1 liefert, a^m aber die niedrigste Potenz von a, welche den kleinsten negativen Rest -1 liefert; so schreiben wir in die zweite Reihe die mit a multiplizirten Zahlen der ersten Reihe und, sobald eine grösser als m werden sollte, deren absolut kleinsten Rest nach dem Model p, also die

Reste von a, $2a$, 2^2a, ... $2^{r-1}a$, in die dritte Reihe die Produkte von a^2, in die vierte die Produkte von a^3 u. s. f., endlich in die letzte der $n = \frac{1}{r} 2^{r-1} = \frac{m}{r}$ Reihen, die Produkte von a^{n-1} mit den Zahlen der ersten Reihe, resp. deren Reste. Die Grundtafel Y ist hiernach

$$\begin{array}{cccccc}
1 & 2 & 2^2 & 2^3 & \ldots & 2^{r-1} \\
a & 2a & 2^2a & 2^3a & \ldots & 2^{r-1}a \\
a^2 & 2a^2 & 2^2a^2 & 2^3a^2 & \ldots & 2^{r-1}a^2 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
a^{n-1} & 2a^{n-1} & 2^2a^{n-1} & 2^3a^{n-1} & \ldots & 2^{r-1}a^{n-1}
\end{array}$$

Die Anfangsglieder 1, a, a^2 ... a^{n-1} der Reihen bilden sich durch Multiplikation mit dem Reste von a, und aus einem Anfangsgliede bildet sich die Horizontalreihe durch fortgesetzte Verdopplung des vorhergehenden Gliedes (unter Vertauschung der erhaltenen Zahl mit ihrem Reste). Sobald also eine primitive Wurzel a bekannt ist, verursacht die Aufstellung der Grundtafel eine sehr geringe Mühe. Eine solche Wurzel ist nach §. 11 leicht zu finden und §. 11 Nr. 2, c lehrt, dass bei der vorausgesetzten Form der Primzahl p die Zahl 3 stets eine solche Wurzel ist (mit Ausnahme des Falles $p = 2^1 + 1 = 3$). Demnach kann man immer $a = 3$ nehmen.

Es ist leicht zu zeigen, dass keine zwei Zahlen $2^b a^c$ und $2^{b'} a^{c'}$, wenn b und $b' < r$ und c und $c' < n$ sind, dieselben kleinsten Reste haben können, dass also alle $m = nr$ Zahlen der Grundtafel verschieden sein oder die Zahlen 1, 2, 3 ... m enthalten werden.

3) Nach dem Zusammenhange der Glieder einer Horizontalreihe reproduziren sich dieselben, wenn man über das letzte (durch Verdopplung des vorhergehenden) hinausschreitet in zyklischer Folge, sodass der Ausdruck Periode für eine solche Reihe gerechtfertigt erscheint und auch ferner für die wirklich periodischen Gruppen von uns gebraucht werden wird.

Schreitet man in der Grundtafel in einer Vertikalreihe 2^b, $2^b a$, $2^b a^2$ ... $2^b a^{n-1}$ durch fortgesetzte Multiplikation mit a abwärts; so muss man beim Überschreiten des letzten Gliedes, also mit dem Reste von $2^b a^n$ nothwendig in das erste Glied 2^c einer anderen Vertikalreihe eintreten, d. h. es muss $2^b a^n \equiv 2^c$ sein. Denn angenommen, man träfe in ein späteres Glied $2^c a^s$ einer solchen Reihe, es wäre also $2^b a^n \equiv 2^c a^s$; so müsste, weil $s < n$ und a relativ prim zu p und zu 2 ist, $2^b a^{n-s} \equiv 2^c$ sein, was aber nur möglich ist, wenn man $s = 0$ hat, da sonst $2^b a^{n-s}$ und 2^c zwei Zahlen aus der Grundtafel sein würden, die nach der Vorbemerkung unbedingt verschieden sein müssen.

Die Vertikalreihe, in welche man beim Überschreiten einer ersten Vertikalreihe einläuft, ist eine andere, als die eben verlassene, weil $2^b a^n$ nicht $\equiv 2^b$ oder a^n nicht $\equiv 1$ sein kann (da nach der Voraussetzung die m-te, also die (nr)-te Potenz von a die niedrigste ist, welche den absolut kleinsten Rest 1 liefert); ausserdem ist sie eine solche, welche um eine unpaare Anzahl von horizontalen Gliedern von der eben verlassenen absteht, d. h. die Differenz $c - b$ oder $b - c$ hat einen unpaaren

Werth. Denn, angenommen, sie hätte einen paaren Werth $2d$, die Kongruenz $2^b a^n \equiv 2^c$ bedingte also, jenachdem b oder c die grössere Zahl ist, entweder die Kongruenz $2^{2d} a^n \equiv 1$, oder die Kongruenz $a^n \equiv 2^{2d}$. Erhebt man die eine oder die andere Kongruenz auf den Grad $\frac{r}{2}$, was immer geschehen kann, da r nach der Voraussetzung eine Potenz von 2, also eine paare Zahl ist; so müsste, weil $2^r \equiv 1$ ist, $a^{\frac{nr}{2}} \equiv 1$ sein, was nicht möglich ist, da die m-te oder (nr)-te Potenz von a die niedrigste ist, welche den absolut kleinsten Rest 1 liefert.

Hiernach bildet eine einzelne Vertikalreihe für sich allein keine zyklische Reihe oder Periode, wohl aber ergiebt sich ein zyklischer Übergang, wenn eine ganze Horizontalreihe in vertikaler Richtung durch Multiplikation aller Glieder mit 3 fortgerückt wird; dieselbe verwandelt sich beim Überschreiten der letzten Horizontalreihe wieder in die erste, jedoch mit verstellten Gliedern.

Ausserdem schliessen sich alle Vertikalreihen zu einer einzigen zyklischen Reihe aneinander, sodass die vertikale Bewegung vom ersten Gliede 1 der Tafel bei abwechselndem Überspringen einer gleichen Anzahl von Reihen endlich zu jenem ersten Gliede wieder zurückkehrt. Auf diesem Wege folgen also die Reste der Potenzen a^0, a^1, a^2, a^3 bis a^{p-1} in natürlicher Reihenfolge der Exponenten aufeinander.

4) Als Beispiel diene die Grundtafel für die Primzahl $p = 2^8 + 1 = 257$, wofür $r = 8$, $m = 128$, $n = 16$ ist, indem wir als primitive Wurzel die Zahl $a = 3$ annehmen. Wir bezeichnen die Horizontalreihen mit den davor gesetzten laufenden Zahlen (0), (1), (2) . . . (15), welche die Exponenten der Potenzen von $a = 3$ anzeigen, deren Reste in den vordersten Gliedern stehen, und die Vertikalreihen bezeichnen wir mit den darüber gesetzten Vielfachen von $2^n = 16$, nämlich mit den Zahlen (0 . 16), (3 . 16), (6 . 16) . . ., welche die Exponenten der Potenzen von a anzeigen, deren Reste in den obersten Gliedern stehen, sodass ein Rest, in welchem sich eine Horizontal- und Vertikalreihe kreuzen, einer Potenz von a entspricht, deren Exponent die Summe der davor und der darüber stehenden Zahl ist. So ist z. B. 66 der Rest der Potenz von 3 vom Exponenten 5 + 7 . 16 = 117. Die Tafel der Reste ist hiernach

	(0 . 16)	(3 . 16)	(6 . 16)	(1 . 16)	(4 . 16)	(7 . 16)	(2 . 16)	(5 . 16)
(0)	1	2	4	8	16	32	64	128
(1)	3	6	12	24	48	96	65	127
(2)	9	18	36	72	113	31	62	124
(3)	27	54	108	41	82	93	71	115
(4)	81	95	67	123	11	22	44	88
(5)	14	28	56	112	33	66	125	7
(6)	42	84	89	79	99	59	118	21
(7)	126	5	10	20	40	80	97	63
(8)	121	15	30	60	120	17	34	68
(9)	106	45	90	77	103	51	102	53

	(0.16)	(3.16)	(6.16)	(1.16)	(4.16)	(7.16)	(2.16)	(5.16)
(10)	61	122	13	26	52	104	49	98
(11)	74	109	39	78	101	55	110	37
(12)	35	70	117	23	46	92	73	111
(13)	105	47	94	69	119	19	38	76
(14)	58	116	25	50	100	57	114	29
(15)	83	91	75	107	43	86	85	87

5) Zu einem aus dem Nachfolgenden ersichtlichen Rechnungszwecke ordnen wir die Grundtafel Y durch Verstellung der Horizontal- und Vertikalreihen jetzt so, dass wir in die obere Hälfte $Y_{\frac{1}{2}}$ die Horizontalreihen mit den paaren Exponenten $2v$ und in die untere Hälfte die Reihen mit den unpaaren Exponenten $2v+1$ setzen. Darauf scheiden wir $Y_{\frac{1}{2}}$ in eine obere Hälfte $Y_{\frac{1}{4}}$ mit den Exponenten $4v$ und eine untere Hälfte $Y_{\frac{2}{4}}$ mit den Exponenten $4v+2$, sowie $Y_{\frac{2}{2}}$ in eine obere Hälfte $Y_{\frac{3}{4}}$ mit den Exponenten $4v+1$ und eine untere Hälfte $Y_{\frac{4}{4}}$ mit den Exponenten $4v+3$. Sodann trennen wir die Gruppen $Y_{\frac{1}{4}}$, $Y_{\frac{2}{4}}$, $Y_{\frac{3}{4}}$, $Y_{\frac{4}{4}}$ resp. in $Y_{\frac{1}{8}}$ und $Y_{\frac{2}{8}}$, $Y_{\frac{3}{8}}$ und $Y_{\frac{4}{8}}$, $Y_{\frac{5}{8}}$ und $Y_{\frac{6}{8}}$, $Y_{\frac{7}{8}}$ und $Y_{\frac{8}{8}}$ resp. mit den Exponenten $8v$ und $8v+4$, $8v+2$ und $8v+6$, $8v+1$ und $8v+5$, $8v+3$ und $8v+7$. Durch fortgesetzte Scheidung gelangt man nach n Scheidungen dahin, dass die Partialgruppen $Y_{\frac{1}{n}}$, $Y_{\frac{2}{n}}$, $Y_{\frac{3}{n}}$ etc. die einzelnen Horizontalreihen darstellen, deren Exponenten in der oberen Hälfte der Tafel resp. die Formen nv, $nv+\frac{n}{2}$, $nv+\frac{n}{4}$, $nv+\frac{n}{2}+\frac{n}{4}$, $nv+\frac{n}{8}$, $nv+\frac{n}{2}+\frac{n}{8}$ etc. und in der unteren Hälfte die Formen $nv+1$, $nv+\frac{n}{2}+1$, $nv+\frac{n}{4}+1$, $nv+\frac{n}{2}+\frac{n}{4}+1$ etc. haben, indem die ersten Glieder dieser Reihen in der oberen Hälfte der Tafel den Exponenten $0, \frac{n}{2}, \frac{n}{4}, \frac{n}{2}+\frac{n}{4}, \frac{n}{8}, \frac{n}{2}+\frac{n}{8}$ etc. und in der unteren Hälfte den Exponenten $1, \frac{n}{2}+1, \frac{n}{4}+1, \frac{n}{2}+\frac{n}{4}+1$ etc. entsprechen.

Hierauf ordnen wir die Vertikalreihen nach demselben Prinzipe, stellen also von den obersten Zahlen, welche den r Potenzen $2^0, 2^1, 2^2 \ldots 2^{r-1}$ der Zahl 2 entsprechen, die Glieder mit paaren Exponenten $2v$ in die vordere und die Glieder mit unpaaren Exponenten $2v+1$

in die hintere Hälfte und verfahren bei der Scheidung dieser Hälften in Viertel hinsichtlich der Exponenten von 2 gerade so wie vorhin hinsichtlich der Exponenten von a. Schliesslich folgen in der obersten Horizontalreihe die einzelnen Potenzen von 2, welche je ein r-tel der ganzen Reihe bilden, so aufeinander, dass ihre Exponenten in der vorderen Hälfte die Reihe $0, \frac{r}{2}, \frac{r}{4}, \frac{r}{2} + \frac{r}{4}$ etc. und in der hinteren Hälfte die Reihe $1, \frac{r}{2} + 1, \frac{r}{4} + 1, \frac{r}{2} + \frac{r}{4} + 1$ etc. bilden. Die geordnete Tafel ist dann die folgende.

	(0.16)	(4.16)	(6.16)	(2.16)	(3.16)	(7.16)	(1.16)	(5.16)
	2^0	2^4	2^2	2^6	2^1	2^5	2^3	2^7
(0)	1	16	4	64	2	32	8	128
(8)	121	120	30	34	15	17	60	68
(4)	81	11	67	44	95	22	123	88
(12)	35	46	117	73	70	92	23	111
(2)	9	113	36	62	18	31	72	124
(10)	61	52	13	49	122	104	26	98
(6)	42	99	89	118	84	59	79	21
(14)	58	100	25	114	116	57	50	29
(1)	3	48	12	65	6	96	24	127
(9)	106	103	90	102	45	51	77	53
(5)	14	33	56	125	28	66	112	7
(13)	105	119	94	38	47	19	69	76
(3)	27	82	108	71	54	93	41	115
(11)	74	101	39	110	109	55	78	37
(7)	126	40	10	97	5	80	20	63
(15)	83	43	75	85	91	86	107	87

6) Fassen wir jetzt die beiden horizontalen Theilgruppen $Y_{\frac{1}{2}}$ und $Y_{\frac{2}{2}}$ ins Auge. Dass dieselben zusammen die Gruppe Y ausmachen, drücken wir durch die Formel $Y_{\frac{1}{2}} + Y_{\frac{2}{2}} = Y$ aus. Denkt man sich jede Zahl der ersten Gruppe zu jeder Zahl der zweiten Gruppe einmal addirt und einmal von ihr subtrahirt; so ergeben sich, weil jede Gruppe $\frac{nr}{2} = 2^{r-2}$ Zahlen enthält, 2^{2r-4} Summen und ebensoviel Differenzen, überhaupt 2^{2r-3} Summen und Differenzen. Wenn wir nur die absoluten Werthe dieser Summen und Differenzen in Betracht ziehen, ausserdem ihre kleinsten absoluten Reste bilden; so können darunter nur die Zahlen 1, 2, 3 ... 2^{r-1} vorkommen. Käme jede dieser Zahlen gleich vielmal vor; so müsste eine jede (2^{r-2})-mal vorkommen. Dass Letzteres der Fall sei, behaupten wir und beweisen es folgendermaassen.

Da $Y_{\frac{1}{2}}$ die Reste der paaren und $Y_{\frac{2}{2}}$ die der unpaaren Potenzen von a enthält; so hat, wenn man in abgekürzter Schreibweise die Potenzen von a für deren Reste setzt, jede Summe die Form $a^{2u+1} + a^{2v}$. Welches auch der Werth dieser Summe sei, immer kann derselbe als der Rest einer Potenz von a, also gleich a^{α} gesetzt werden, man hat also

$$a^{2u+1} + a^{2v} = a^{\alpha}$$

Multipliziren wir diese Gleichung mit a^{m-2v}; so kömmt, da a^m den Rest 1 hat, also entweder $\equiv +1$, oder $\equiv -1$ ist,

$$a^{m+2u-2v+1} \pm 1 = a^{m+\alpha-2v} = a^{w}$$

Nehmen wir zuvörderst an, es gelte das obere Zeichen. Welchen Werth auch die rechte Seite a^w habe, indem man die Gleichung sukzessiv mit den aufsteigenden Potenzen von a multiplizirt, stellen die rechten Seiten a^w, a^{w+1}, a^{w+2}, ... a^{w+m-1} sämmtliche m Zahlen 1, 2, 3 ... m (in irgend einer Reihenfolge) dar, während die linken Seiten die Werthe

$$\begin{aligned} &a^{m+2u-2v+1} + 1 \\ &a^{m+2u-2v+2} + a^1 \\ &a^{m+2u-2v+3} + a^2 \\ &a^{m+2u-2v+4} + a^3 \end{aligned}$$

etc.

annehmen. Man erkennt hierin die Summen von zwei Zahlen der oberen und der unteren Theilgruppe, welche von den ursprünglichen Stellen aus immer um eine bestimmte Stellenzahl sich verschieben, bis sie nach m Verschiebungen wieder in die ursprünglichen Stellen treffen. Bei der Ersetzung einer Potenz, welche das Glied einer Summe bildet, durch ihren kleinsten absoluten Rest, muss, um die Gleichheit der linken und rechten Seite zu erhalten, zuvörderst das Zeichen dieses Restes beibehalten werden: erst nach der Vereinigung beider Glieder kann das Zeichen der Summe als unwesentlich unterdrückt werden. Hierdurch kann und wird es kommen, dass die Zeichen der beiden Glieder bald übereinstimmen, bald einander entgegengesetzt sind, oder mit anderen Worten, dass die beiden Glieder auf der linken Seite bald eine Summe, bald eine Differenz zweier Zahlen der oberen und unteren Theilgruppe bilden.

Der Werth dieser Summen und Differenzen variirt mit dem Werthe von $2u - 2v$ und diese Zahl kann $\frac{1}{2}m$ verschiedene Werthe annehmen.

Ganz das Nämliche gilt, wenn man an die Stelle der Summe $a^{2u+1} + a^{2v}$ die Differenz $a^{2u+1} - a^{2v} = a^{\beta}$ setzt.

Ferner leuchtet ein, dass sobald eine Summe durch die Negativität eines Restes sich in eine Differenz verwandelt, auch die Differenz mit den gleichen Exponenten sich in eine Summe verwandelt, dass also im Ganzen $\frac{1}{2}m$ wirkliche Summen und ebenso viel wirkliche Differenzen, überhaupt m Summen und Differenzen erscheinen. Eine jede dieser Summen und Differenzen liefert durch die Multiplikation mit a^0, a^1, a^2 ... a^{m-1} eine

jede der Zahlen 1, 2, 3 ... m: allein es wiederholt sich bei dieser Multiplikation mit allen jenen Summen und Differenzen jeder Fall zweimal (denn $a^\gamma + a^\delta$ liefert bei der Multiplikation mit a^0, a^1, a^2 ... a^m ganz dieselben Glieder wie $a^{m-\gamma} + a^{m-\delta}$, wobei nur das Vorder- und Hinterglied ihre Stelle vertauschen). Demzufolge wird jede der Zahlen 1, 2, 3 ... m nicht m-mal, sondern $\frac{1}{2}\,m$- $= (2^{r-2})$-mal in jenen Summen und Differenzen zum Vorschein kommen, wie zu beweisen war.

Wenn a^m nicht, wie angenommen, $\equiv +1$, sondern $\equiv -1$ ist, gilt in der Formel, auf welche sich die vorstehende Entwicklung stützt, das untere Zeichen. In Folge dessen verwandelt sich jede Summe in eine Differenz und jede Differenz in eine Summe, was schliesslich zu demselben Resultate führt.

Stellen wir die Operation der Addition und Subtraktion aller Glieder der Gruppe $Y_{\frac{1}{2}}$ mit allen Gliedern der Gruppe $Y_{\frac{2}{2}}$ dadurch dar, dass wir die Symbole beider Gruppen nebeneinander stellen; so haben wir nach Vorstehendem die Formel

$$Y_{\frac{1}{2}}\ Y_{\frac{2}{2}} = 2^{r-2}\ Y$$

Für das Beispiel $p = 257$ ist $2^{r-2} = 64$, also

$$Y_{\frac{1}{2}}\ Y_{\frac{2}{2}} = 64\ Y$$

7) Für die horizontalen Theilgruppen $Y_{\frac{1}{4}}$, $Y_{\frac{2}{4}}$, sowie $Y_{\frac{3}{4}}$, $Y_{\frac{4}{4}}$ haben wir zunächst die Beziehungen

$$Y_{\frac{1}{4}} + Y_{\frac{2}{4}} = Y_{\frac{1}{2}} \qquad Y_{\frac{3}{4}} + Y_{\frac{4}{4}} = Y_{\frac{2}{2}}$$

Kombiniren wir die ersteren beiden Gruppen $Y_{\frac{1}{4}}$ und $Y_{\frac{2}{4}}$ durch Addition und Subtraktion der Glieder; so ergiebt eine Addition Glieder von der Form

$$a^{4u+2} + a^{4v} = a^\alpha$$

und nach Multiplikation mit a^{m-4v}, wodurch sich offenbar immer die Summe zweier Glieder derselben Gruppen ergiebt;

$$a^{m+4u-4v+2} + 1 = a^{m+\alpha-4v} = a^w$$

Welchen Werth auch a^w habe, immer liefert eine Multiplikation mit den sukzessiven paaren Potenzen von a, also mit a^0, a^2 a^4 ... a^{m-2} auf der rechten Seite als Reste von a^w, a^{w+2}, a^{w+4}, ... a^{w+m-2} sämmtliche Zahlen einer bestimmten der beiden Gruppen $Y_{\frac{1}{2}}$ und $Y_{\frac{2}{2}}$, nämlich die Zahlen der Gruppe $Y_{\frac{1}{2}}$, wenn α (und daher auch w) paar ist, und die Zahlen der Gruppe $Y_{\frac{2}{2}}$, wenn α (und daher auch w) unpaar ist, während auf der linken Seite die Summen

$$\begin{aligned} &a^{m+4u-4v+2} + 1 \\ &a^{m+4u-4v+4} + a^2 \\ &a^{m+4u-4v+6} + a^4 \\ &a^{m+4u-4v+8} + a^6 \end{aligned}$$

etc.

von je einer Zahl der Gruppe $Y_{\frac{1}{4}}$ und $Y_{\frac{2}{4}}$ erscheinen. Auch hier verwandelt sich, sobald eins der beiden Glieder einen negativen Rest liefert, die Summe in eine Differenz. Der Werth dieser Summen und Differenzen variirt mit dem Werthe von $4u - 4v$ und kann daher $\frac{1}{4}m$ verschiedene Werthe annehmen.

Ganz das Nämliche gilt von der Differenz $a^{4u+2} - a^{4v} = a^{\beta}$. Jenachdem β paar oder unpaar ist, stellen diese Differenzen (von welchen sich ebenso viel in Summen verwandeln, als sich vorher Summen in Differenzen verwandelten) Reste der Gruppe $Y_{\frac{1}{2}}$ oder der Gruppe $Y_{\frac{2}{2}}$ dar, sodass man $\frac{1}{4}m$ wirkliche Summen und $\frac{1}{4}m$ wirkliche Differenzen, überhaupt $\frac{1}{2}m$ Summen und Differenzen erhält. Eine jede derselben liefert durch die Multiplikation mit den paaren Potenzen von a eine jede der Zahlen der betreffenden Gruppe, wobei sich jedoch jeder Fall unter Vertauschung des Vorder- und Hintergliedes einmal wiederholt, sodass jede der ebengedachten Zahlen nicht $\frac{1}{2}m$-, sondern $\frac{1}{4}m$-mal zum Vorschein kömmt. Bildet man nämlich die durch Multiplikation aus jeder der Zahlen $a^2 + 1$, $a^6 + 1$, $a^{10} + 1$, ... a^{m-2} mit jeder der Potenzen a^0, a^2, a^4 ... a^{m-2} sich ergebenden Produkte; so erhält man, indem man beachtet, dass $m - 2 = 4\left(\frac{m}{4} - 1\right) + 2$ ist,

$a^2 + 1$	$a^6 + 1$	$a^{10} + 1$	...	$a^{m-2} + 1$
$a^4 + a^2$	$a^8 + a^2$	$a^{12} + a^2$	...	$a^m + a^2$
$a^6 + a^4$	$a^{10} + a^4$	$a^{14} + a^4$	...	$a^{m+2} + a^4$
.	.	.		.
.	.	.		.
.	.	.		.
$a^{m-2} + a^{m-4}$	$a^{m+2} + a^{m-4}$	$a^{m+6} + a^{m-4}$	...	$a^{2m-6} + a^{m-4}$
$a^m + a^{m-2}$	$a^{m+4} + a^{m-2}$	$a^{m+8} + a^{m-2}$	...	$a^{2m-4} + a^{m-2}$

Ähnliche Produkte ergeben sich aus den Differenzen $a^2 - 1$, $a^6 - 1$, $a^{10} - 1$ etc. Wenn $a^m \equiv 1$ ist; so enthält die letzte vertikale Reihe von Produkten dieselben Zahlen wie die erste, die vorletzte wie die zweite,

die drittletzte wie die dritte u. s. w., sodass nur die ersten $\frac{m}{8}$ Reihen, deren letzte mit $a^{\frac{m}{2}-2} + 1$ beginnt, in Betracht kommen. Dasselbe gilt von den Differenzen. Wenn aber $a^m \equiv -1$ ist; so verwandelt sich die letzte Reihe vom zweiten Produkte an in Differenzen, während in der ersten Reihe nur das letzte Produkt eine Differenz wird. In der vorletzten Reihe werden alsdann die Produkte vom vierten an Differenzen, während in der zweiten Reihe die untersten drei Summen zu Differenzen werden u. s. f. Ähnlich verwandeln sich die Differenzen in Summen.

In allen Fällen brauchen nur die ersten $\frac{m}{8}$ Reihen als Summen und als Differenzen in Betracht gezogen zu werden. Wenn in einer solchen Reihe irgend eine Zahl, z. B. die erste, welche die Form $a^{4w+2} \pm 1$ hat, gleich a^w ist; so wird, jenachdem w paar oder unpaar ist, auch für jede andere Zahl dieser Reihe, wenn sie $= a^v$ gesetzt wird, der Exponent w resp. paar oder unpaar sein. Hiernach kömmt es lediglich darauf an, die Werthe festzustellen, welche w für die $\frac{m}{4}$ Zahlen

$$a^2 \pm 1 \qquad a^6 \pm 1 \qquad a^{10} \pm 1 \qquad \ldots a^{\frac{m}{2}-2} \pm 1$$

annimmt. Angenommen, hierunter habe w im Ganzen k_2- mal einen paaren und k_3- mal einen unpaaren Werth; so ergiebt sich ohne Weiteres

$$Y_{\frac{1}{4}}\ Y_{\frac{2}{4}} = k_2\ Y_{\frac{1}{2}} + k_3\ Y_{\frac{2}{2}}$$

Hierin ist $k_2 + k_3 = \frac{m}{4} = 2^{r-3}$.

Wäre $k_2 = k_3 = \frac{m}{8}$; so hätte man

$$Y_{\frac{1}{4}}\ Y_{\frac{2}{4}} = 2^{r-4}\ Y$$

Die Bestimmung der Werthe von w ist mit Hülfe der in Nr. 5 aufgestellten Tafel, in welcher die Exponenten der verschiedenen Reste aus den davor und darüber gesetzten eingeklammerten Zahlen zu ersehen sind, eine leichte mechanische Arbeit. Da w und $w' = w - x \cdot n$ zugleich paar oder unpaar sind; so braucht man nicht die wirklichen Werthe von w, sondern nur die vor den horizontalen Perioden stehenden eingeklammerten Exponenten w' zu kennen, also nur die Perioden zu ermitteln, in welchen die in Rede stehenden Summen und Differenzen liegen. Für das Beispiel $p = 257$ erhält man folgende Zusammenstellung

Summe der Reste	Betrag	Exponent w'	Differenz der Reste	Betrag	Exponent w'
$a^2 + 1$	10	7	$a^2 - 1$	8	0
$a^6 + 1$	43	15	$a^6 - 1$	41	3
$a^{10} + 1$	62	2	$a^{10} - 1$	60	8
$a^{14} + 1$	59	6	$a^{14} - 1$	57	14
$a^{18} + 1$	73	12	$a^{18} - 1$	71	3
$a^{22} + 1$	80	7	$a^{22} - 1$	78	11
$a^{26} + 1$	27	3	$a^{26} - 1$	25	14
$a^{30} + 1$	51	9	$a^{30} - 1$	49	10
$a^{34} + 1$	63	7	$a^{34} - 1$	61	10
$a^{38} + 1$	119	13	$a^{38} - 1$	117	12
$a^{42} + 1$	50	14	$a^{42} - 1$	48	1
$a^{46} + 1$	115	3	$a^{46} - 1$	113	2
$a^{50} + 1$	19	13	$a^{50} - 1$	17	8
$a^{54} + 1$	85	15	$a^{54} - 1$	83	15
$a^{58} + 1$	123	4	$a^{58} - 1$	121	8
$a^{62} + 1$	117	12	$a^{62} - 1$	115	3

Diese Zusammenstellung enthält 16 paare und 16 unpaare Werthe von w', man hat also $k_2 = k_3 = 16$ und daher

$$Y_{\frac{1}{4}} \; Y_{\frac{2}{4}} = 16 \; Y$$

Kombiniren wir jetzt die beiden Gruppen $Y_{\frac{3}{4}}$ und $Y_{\frac{4}{4}}$; so ist die allgemeine Form einer Summe oder Differenz

$$a^{4u+3} \pm a^{4v+1} = a^{\alpha}$$

$$(a^{m+4u-4v+2} \pm 1)\, a = a^{m+\alpha-4v+1} = a^{w+1}$$

Multiplizirt man jede dieser Form entsprechende Zahl mit jeder der paaren Potenzen a^0, a^2, $a^4 \ldots a^{m-2}$; so ergeben sich die jetzt gesuchten Summen und Differenzen. Dieselben ergeben sich aus den obigen, wenn man diese mit a multiplizirt, in der Form

$$(a^2 \pm 1)\, a \qquad (a^6 + 1)\, a \qquad \ldots \; (a^{\frac{m}{2}-2} + 1)\, a$$

$$(a^4 \pm a^2)\, a \qquad (a^8 + a^2)\, a \qquad (a^{\frac{m}{2}} + a^2)\, a$$

$$\vdots \qquad \vdots \qquad \vdots$$

Hieraus geht hervor, dass die Exponenten $w + 1$ um eine Einheit grösser sind, als die früheren Exponenten w, oder dass die früher paaren jetzt unpaar und die früher unpaaren jetzt paar werden, dass also die beiden Koeffizienten k_2 und k_3 ihre Werthe vertauschen. Demnach ist

$$Y_{\frac{3}{4}}\ Y_{\frac{4}{4}} = k_3\ Y_{\frac{1}{2}} + k_2\ Y_{\frac{2}{2}}$$

Wenn $k_2 = k_3 = \frac{m}{8} = 2^{r-4}$ ist, wird

$$Y_{\frac{3}{4}}\ Y_{\frac{4}{4}} = 2^{r-4}\ Y$$

So ist z. B. für $p = 257$, $k_2 = k_3 = 16$, also

$$Y_{\frac{3}{4}}\ Y_{\frac{4}{4}} = 16\ Y$$

Die Summe der beiden Kombinationen ist allgemein

$$Y_{\frac{1}{4}}\ Y_{\frac{2}{4}} + Y_{\frac{3}{4}}\ Y_{\frac{4}{4}} = 2^{r-3}\ Y$$

also für $p = 257$ gleich $32\ Y$.

8) Für die Theilgruppen $Y_{\frac{1}{8}}$, $Y_{\frac{2}{8}}$ etc. hat man zunächst

$$Y_{\frac{1}{8}} + Y_{\frac{2}{8}} = Y_{\frac{1}{4}} \qquad Y_{\frac{3}{8}} + Y_{\frac{4}{8}} = Y_{\frac{2}{4}} \qquad Y_{\frac{5}{8}} + Y_{\frac{6}{8}} = Y_{\frac{3}{4}}$$
$$Y_{\frac{7}{8}} + Y_{\frac{8}{8}} = Y_{\frac{4}{4}}$$

Eine Kombination von $Y_{\frac{1}{8}}$ und $Y_{\frac{2}{8}}$ giebt

$$a^{8u+4} \pm a^{8v} = a^{\alpha}$$
$$a^{m+8u-8v+4} \pm 1 = a^{m+\alpha-8v} = a^{w}$$

Multiplizirt man jede der $\frac{m}{8}$ Zahlen $a^4 \pm 1$, $a^{12} \pm 1$, $a^{20} \pm 1 \ldots a^{\frac{m}{2}-4} \pm 1$ mit jeder der $\frac{m}{4}$ Potenzen $a^0\ a^4$, a^8, $a^{12} \ldots a^{m-4}$; so ergeben sich die Produkte

a^4	± 1	a^{12}	± 1	a^{20}	± 1	$\ldots\ a^{\frac{m}{2}-4}$	± 1
a^8	$\pm a^4$	a^{16}	$\pm a^4$	a^{24}	$\pm a^4$	$a^{\frac{m}{2}}$	$\pm a^4$
a^{12}	$\pm a^8$	a^{20}	$\pm a^8$	a^{28}	$\pm a^8$	$a^{\frac{m}{2}+4}$	$\pm a^8$
.		.		.		.	
.		.		.		.	
.		.		.		.	
a^m	$\pm a^{m-4}$	a^{m+8}	$\pm a^{m-4}$	a^{m+16}	$\pm a^{m-4}$	$a^{\frac{3m}{2}-8}$	$\pm a^{m-4}$

Jenachdem die oberste Zahl einer dieser Vertikalreihen einer Potenz von der Form a^{4w}, a^{4w+2}, a^{4w+1}, a^{4w+3} äquivalent ist, stellen die $\frac{m}{4}$ Zahlen dieser Reihe alle Zahlen resp. der Gruppe $Y_{\frac{1}{4}}$, $Y_{\frac{2}{4}}$, $Y_{\frac{3}{4}}$, $Y_{\frac{4}{4}}$ dar. Kömmt also unter den $\frac{m}{8}$ Summen und Differenzen, welche in den obersten Stellen stehen, der Exponent der äquivalenten Potenzen k_4-mal in der Form $4w$, k_5-mal in der Form $4w+2$, k_6-mal in der Form $4w+1$ und k_7-mal in der Form $4w+3$ vor, sodass $k_4 + k_5 + k_6 + k_7 = \frac{m}{8} = 2^{r-4}$ ist; so hat man

$$Y_{\frac{1}{8}}\, Y_{\frac{2}{8}} = k_4\, Y_{\frac{1}{4}} + k_5\, Y_{\frac{2}{4}} + k_6\, Y_{\frac{3}{4}} + k_7\, Y_{\frac{4}{4}}$$

Die Kombination von $Y_{\frac{3}{8}}$ und $Y_{\frac{4}{8}}$ giebt

$$a^{8u+6} \pm a^{8u+2} = (a^{8u+4} \pm a^{8v})\, a^2$$

Diese Zahlen sind die Produkte der vorhergehenden mit a^2, die Exponenten erhöhen sich also um 2, wodurch sich k_4 in k_5, k_5 in k_4, k_6 und k_7 und k_7 in k_6 verwandelt. Hieraus folgt

$$Y_{\frac{3}{8}}\, Y_{\frac{4}{8}} = k_5\, Y_{\frac{1}{4}} + k_4\, Y_{\frac{2}{4}} + k_7\, Y_{\frac{3}{4}} + k_6\, Y_{\frac{4}{4}}$$

Die Kombination von $Y_{\frac{5}{8}}$ und $Y_{\frac{6}{8}}$ giebt

$$a^{8u+5} \pm a^{8u+1} = (a^{8u+4} \pm a^{8u})\, a$$

Diese Zahlen sind die Produkte der ersten mit a, die Exponenten erhöhen sich also um 1, wodurch sich k_4 in k_6, k_5 in k_7, k_6 in k_5 und k_7 in k_4 verwandelt. Hieraus folgt

$$Y_{\frac{5}{8}}\, Y_{\frac{6}{8}} = k_6\, Y_{\frac{1}{4}} + k_7\, Y_{\frac{2}{4}} + k_5\, Y_{\frac{3}{4}} + k_4\, Y_{\frac{4}{4}}$$

Die Kombination von $Y_{\frac{7}{8}}$ und $Y_{\frac{8}{8}}$ giebt

$$a^{8u+7} \pm a^{8u+3} = (a^{8u+4} \pm a^{8u})\, a^3$$

Diese Zahlen sind die Produkte der ersten mit a^3, die Exponenten erhöhen sich also um 3, wodurch sich k_4 in k_7, k_5 in k_6, k_6 in k_4 k_7 in k_5 verwandelt. Hieraus folgt

$$Y_{\frac{7}{8}}\, Y_{\frac{8}{8}} = k_7\, Y_{\frac{1}{4}} + k_6\, Y_{\frac{2}{4}} + k_4\, Y_{\frac{3}{4}} + k_5\, Y_{\frac{4}{4}}$$

In allen diesen Formeln ist $k_4 + k_5 + k_6 + k_7 = \frac{m}{8} = 2^{r-4}$. Wäre $k_4 = k_5 = k_6 = k_7 = 2^{r-6}$; so hätte man

$$Y_{\frac{1}{8}}\, Y_{\frac{2}{8}} = Y_{\frac{3}{8}}\, Y_{\frac{4}{8}} = Y_{\frac{5}{8}}\, Y_{\frac{6}{8}} = Y_{\frac{7}{8}}\, Y_{\frac{8}{8}} = 2^{r-6}\, Y$$

Für das Beispiel $p = 257$ liefert die Tafel in Nr. 5 folgende Zusammenstellung der Summen und Reste von der Form

$$a^{8u+4} \pm 1 = a^{w'+xn}$$

Summe der Reste	Betrag	Exponent w'	Differenz der Reste	Betrag	Exponent w'
$a^4 + 1$	82	3	$a^4 - 1$	80	7
$a^{12} + 1$	36	2	$a^{12} - 1$	34	8
$a^{20} + 1$	124	2	$a^{20} - 1$	122	10
$a^{28} + 1$	24	1	$a^{28} - 1$	22	4
$a^{36} + 1$	45	9	$a^{36} - 1$	43	15
$a^{44} + 1$	74	11	$a^{44} - 1$	72	2
$a^{52} + 1$	96	1	$a^{52} - 1$	94	13
$a^{64} + 1$	71	3	$a^{64} - 1$	69	13

Unter den Exponenten w' kommen vor von der Form

$4v$	die Werthe 8, 4	es ist also	$k_4 = 2$
$4v + 2$	„ „ 2, 2, 10, 2	„ „ „	$k_5 = 4$
$4v + 1$	„ „ 1, 9, 1, 13, 13	„ „ „	$k_6 = 5$
$4v + 3$	„ „ 3, 3, 3, 7, 15	„ „ „	$k_7 = 5$

Hiernach hat man

$$Y_{\frac{1}{8}}\, Y_{\frac{2}{8}} = 2\, Y_{\frac{1}{4}} + 4\, Y_{\frac{2}{4}} + 5\, Y_{\frac{3}{4}} + 5\, Y_{\frac{4}{4}}$$

$$Y_{\frac{3}{8}}\, Y_{\frac{4}{8}} = 4\, Y_{\frac{1}{4}} + 2\, Y_{\frac{2}{4}} + 5\, Y_{\frac{3}{4}} + 5\, Y_{\frac{4}{4}}$$

$$Y_{\frac{5}{8}}\, Y_{\frac{6}{8}} = 5\, Y_{\frac{1}{4}} + 5\, Y_{\frac{2}{4}} + 4\, Y_{\frac{3}{4}} + 2\, Y_{\frac{4}{4}}$$

$$Y_{\frac{7}{8}}\, Y_{\frac{8}{8}} = 5\, Y_{\frac{1}{4}} + 5\, Y_{\frac{2}{4}} + 2\, Y_{\frac{3}{4}} + 4\, Y_{\frac{4}{4}}$$

Die Summe dieser vier Kombinationen ist allgemein

$$Y_{\frac{1}{8}}\, Y_{\frac{2}{8}} + Y_{\frac{3}{8}}\, Y_{\frac{4}{8}} + Y_{\frac{5}{8}}\, Y_{\frac{6}{8}} + Y_{\frac{7}{8}}\, Y_{\frac{8}{8}} = 2^{r-4}\, Y$$

also für $p = 257$ gleich $16\, Y$.

9) Für die Theilgruppen $Y_{\frac{1}{16}}$, $Y_{\frac{2}{16}}$ etc. hat man

$$Y_{\frac{1}{16}} + Y_{\frac{2}{16}} = Y_{\frac{1}{8}} \qquad Y_{\frac{3}{16}} + Y_{\frac{4}{16}} = Y_{\frac{2}{8}} \text{ etc.}$$

Eine Kombination von $Y_{\frac{1}{16}}$ und $Y_{\frac{2}{16}}$ giebt

$$a^{16u+8} \pm a^{16v} = a^{\alpha}$$
$$a^{m+16u-16v+8} \pm 1 = a^{m+\alpha-16v} = a^{w}$$

Multiplizirt man jede der $\frac{m}{16}$ Zahlen $a^{8} \pm 1$, $a^{24} \pm 1$, $a^{40} \pm 1 \ldots a^{\frac{m}{2}-8}$ mit jeder der $\frac{m}{8}$ Potenzen a^{0}, a^{8}, $a^{16} \ldots a^{m-8}$; so ergeben sich die Produkte

a^{8}	± 1	a^{24}	± 1	a^{40}	± 1	$\ldots\ a^{\frac{m}{2}-8}$	± 1
a^{16}	$\pm a^{8}$	a^{32}	$\pm a^{8}$	a^{48}	$\pm a^{8}$	$a^{\frac{m}{2}}$	$\pm a^{8}$
a^{24}	$\pm a^{16}$	a^{40}	$\pm a^{16}$	a^{56}	$\pm a^{16}$	$a^{\frac{m}{2}+8}$	$\pm a^{16}$
.		.		.		.	
.		.		.		.	
.		.		.		.	
a^{m}	$\pm a^{m-8}$	a^{m+16}	$\pm a^{m-8}$	a^{m+32}	$\pm a^{m-8}$	$a^{\frac{3m}{2}-16}$	$\pm a^{m-8}$

Jenachdem die oberste Zahl einer dieser Vertikalreihen einer Potenz von der Form a^{8w}, a^{8w+4}, a^{8w+2}, a^{8w+6}, a^{8w+1}, a^{8w+5}, a^{8w+3}, a^{8w+7} äquivalent ist, stellen die $\frac{m}{8}$ Zahlen dieser Reihe alle Zahlen resp. der Gruppe $Y_{\frac{1}{8}}$, $Y_{\frac{2}{8}}$, $Y_{\frac{3}{8}}$, $Y_{\frac{4}{8}}$, $Y_{\frac{5}{8}}$, $Y_{\frac{6}{8}}$, $Y_{\frac{7}{8}}$, $Y_{\frac{8}{8}}$ dar. Kömmt also unter den $\frac{m}{16}$ Summen und Differenzen, welche in den obersten Stellen stehen, der Exponent der äquivalenten Potenzen resp. k_8-, k_9-, k_{10}-, k_{11}-, k_{12}-, k_{13}-, k_{14}-, k_{15}-mal in der Form $8w$, $8w+4$, $8w+2$, $8w+6$, $8w+1$, $8w+5$, $8w+3$, $8w+7$ vor, sodass $k_8 + k_9 + \ldots + k_{15} = \frac{m}{16} = 2^{r-5}$ ist, so hat man

$$Y_{\frac{1}{16}}\ Y_{\frac{2}{16}} = k_8\ Y_{\frac{1}{8}} + k_9\ Y_{\frac{2}{8}} + k_{10}\ Y_{\frac{3}{8}} + k_{11}\ Y_{\frac{4}{8}} + k_{12}\ Y_{\frac{5}{8}} + k_{13}\ Y_{\frac{6}{8}} + k_{14}\ Y_{\frac{7}{8}} + k_{15}\ Y_{\frac{8}{8}}$$

Aus dieser Kombination ergeben sich die folgenden $Y_{\frac{3}{16}}\ Y_{\frac{4}{16}}$, $Y_{\frac{5}{16}}\ Y_{\frac{6}{16}}$ etc. durch Multiplikation resp. mit a^4, a^2, a^6, a, a^5, a^3, a^7, und die Zeiger der Koeffizienten k nehmen folgende Werthe an

in $Y_{\frac{1}{16}}$	$Y_{\frac{2}{16}}$	8	9	10	11	12	13	14	15
$Y_{\frac{3}{16}}$	$Y_{\frac{4}{16}}$	9	8	11	10	13	12	15	14
$Y_{\frac{5}{16}}$	$Y_{\frac{6}{16}}$	10	11	9	8	14	15	13	12
$Y_{\frac{7}{16}}$	$Y_{\frac{8}{16}}$	11	10	8	9	15	14	12	13
$Y_{\frac{9}{16}}$	$Y_{\frac{10}{16}}$	12	13	14	15	10	11	9	8
$Y_{\frac{11}{16}}$	$Y_{\frac{12}{16}}$	13	12	15	14	11	10	8	9
$Y_{\frac{13}{16}}$	$Y_{\frac{14}{16}}$	14	15	13	12	9	8	11	10
$Y_{\frac{15}{16}}$	$Y_{\frac{16}{16}}$	15	14	12	13	8	9	10	11

Die Summe aller dieser 8 Kombinationen ist gleich $2^{r-5}\ Y$, z. B. für $p = 257$ gleich $8\ Y$.

Für das Beispiel $p = 257$ liefert die Tafel in Nr. 5 folgende Zusammenstellung

Summe der Reste	Betrag	Exponent w'	Summe der Differenzen	Betrag	Exponent w'
$a^8 + 1$	122	10	$a^8 - 1$	120	8
$a^{24} + 1$	61	10	$a^{24} - 1$	59	6
$a^{40} + 1$	35	12	$a^{40} - 1$	33	5
$a^{56} + 1$	16	0	$a^{56} - 1$	14	5

Unter den Exponenten w' befinden sich von der Form

$8v$	die Werthe 0, 8	es ist also	$k_8 = 2$
$8v + 4$	„ „ 12	„ „ „	$k_9 = 1$
$8v + 2$	„ „ 10, 10	„ „ „	$k_{10} = 2$
$8v + 6$	„ „ 6	„ „ „	$k_{11} = 1$
$8v + 5$	„ „ 5	„ „ „	$k_{13} = 2$

Die übrigen drei Koeffizienten k_{12}, k_{14}, k_{15} sind gleich null. Diess giebt

$$
\begin{aligned}
Y_{\frac{1}{16}}\, Y_{\frac{2}{16}} &= 2\,Y_{\frac{1}{8}} + Y_{\frac{2}{8}} + 2\,Y_{\frac{3}{8}} + Y_{\frac{4}{8}} + 2\,Y_{\frac{6}{8}}\\
Y_{\frac{3}{16}}\, Y_{\frac{4}{16}} &= Y_{\frac{1}{8}} + 2\,Y_{\frac{2}{8}} + Y_{\frac{3}{8}} + 2\,Y_{\frac{4}{8}} + 2\,Y_{\frac{5}{8}}\\
Y_{\frac{5}{16}}\, Y_{\frac{6}{16}} &= 2\,Y_{\frac{1}{8}} + Y_{\frac{2}{8}} + Y_{\frac{3}{8}} + 2\,Y_{\frac{4}{8}} + 2\,Y_{\frac{7}{8}}\\
Y_{\frac{7}{16}}\, Y_{\frac{8}{16}} &= Y_{\frac{1}{8}} + 2\,Y_{\frac{2}{8}} + 2\,Y_{\frac{3}{8}} + Y_{\frac{4}{8}} + 2\,Y_{\frac{8}{8}}\\
Y_{\frac{9}{16}}\, Y_{\frac{10}{16}} &= 2\,Y_{\frac{2}{8}} + 2\,Y_{\frac{5}{8}} + Y_{\frac{6}{8}} + Y_{\frac{7}{8}} + 2\,Y_{\frac{8}{8}}\\
Y_{\frac{11}{16}}\, Y_{\frac{12}{16}} &= 2\,Y_{\frac{1}{8}} + Y_{\frac{5}{8}} + 2\,Y_{\frac{6}{8}} + 2\,Y_{\frac{7}{8}} + Y_{\frac{8}{8}}\\
Y_{\frac{13}{16}}\, Y_{\frac{14}{16}} &= 2\,Y_{\frac{3}{8}} + Y_{\frac{5}{8}} + 2\,Y_{\frac{6}{8}} + Y_{\frac{7}{8}} + 2\,Y_{\frac{8}{8}}\\
Y_{\frac{15}{16}}\, Y_{\frac{16}{16}} &= 2\,Y_{\frac{4}{8}} + 2\,Y_{\frac{5}{8}} + Y_{\frac{6}{8}} + 2\,Y_{\frac{7}{8}} + Y_{\frac{8}{8}}
\end{aligned}
$$

10) Da $r = 2^s$, also $n = 2^{r-s-1}$ ist; so stösst man bei $r - s - 1$ Halbirungen auf die einzelnen Perioden $Y_{\frac{1}{n}}$, $Y_{\frac{2}{n}}$, $Y_{\frac{3}{n}}$ etc. Für $p = 257$, also $r = 8$, $s = 3$, $r - s - 1 = 4$, $n = 16$, erfolgt Diess nach 4 Halbirungen, wodurch sich die einzelnen Perioden $Y_{\frac{1}{16}}$, $Y_{\frac{2}{16}}$ etc. ergeben, wie bereits in der vorstehenden Nummer geschehen.

11) Nachdem Diess erreicht ist, beginnen wir die einzelnen Perioden durch fortgesetzte Halbirung zu zerlegen. Die Zerlegung der ersten Periode genügt, um daraus unmittelbar die Zerlegungen aller übrigen n Perioden abzuleiten. Diese erste Periode $Y_{\frac{1}{n}}$ enthält r Potenzen von 2 nach der in Nr. 5 beschriebenen Anordnung. In der linken Hälfte, welche wir mit $Y_{\frac{1}{n}\cdot\frac{1}{2}}$ bezeichnen, stehen die geraden Potenzen 2^{2v}, in der rechten Hälfte, welche wir mit $Y_{\frac{1}{n}\cdot\frac{2}{2}}$ bezeichnen, die ungeraden Potenzen 2^{2u+1}; man hat

$$Y_{\frac{1}{n}\cdot\frac{1}{2}} + Y_{\frac{1}{n}\cdot\frac{2}{2}} = Y_{\frac{1}{n}}$$

und behuf der Kombination $Y_{\frac{1}{n}\cdot\frac{1}{2}}\ Y_{\frac{1}{n}\cdot\frac{2}{2}}$ sind die Zahlen

$$2^{2u+1} \pm 2^{2v} = a^{\alpha}$$

zu bilden. Welches nun auch der Werth von a für irgend welche Werthe von u und v sein mag, eine sukzessive Multiplikation dieser Gleichung mit den r Potenzen $2^0, 2^1, 2^2 \ldots 2^{r-1}$ liefert die r Glieder einer bestimmten Periode. Die ganze Kombination, welche $2\,\frac{r}{2}\cdot\frac{r}{2} = \frac{1}{2}\,r^2$ Zahlen enthält, wird also $\frac{r}{2}$ Perioden in sich fassen. Dieselben ergeben

sich, wenn man folgende $\frac{r}{2}$ Zahlen von der Form $2^{2^u+1} \pm 1$

$$2 \pm 1 \qquad 2^3 \pm 1 \qquad 2^5 \pm 1 \ldots 2^{\frac{r}{2}-1} \pm 1$$

bildet und in der Tafel von Nr. 5 nachsieht, welchen Potenzen a^w diese Summen entsprechen. Da $w = w' + xn$ ist; so braucht man nur den Werth von w' zu ermitteln, um die Periode zu bestimmen, welcher die betreffende Snmme oder Differenz angehört. Kömmt die Periode $Y_{\frac{1}{n}}$ l_1-mal, die Periode $Y_{\frac{2}{n}}$ l_2-mal, die Periode $Y_{\frac{3}{n}}$ l_3-mal u. s. w. vor; so wird

$$Y_{\frac{1}{n}} \cdot Y_{\frac{1}{n}}^{\frac{1}{2}} \cdot Y_{\frac{2}{n}}^{\frac{2}{2}} = l_1 Y_{\frac{1}{n}} + l_2 Y_{\frac{2}{n}} + l_3 Y_{\frac{3}{n}} + \ldots + l_n Y_{\frac{n}{n}}$$

worin $l_1 + l_2 + l_3 + \ldots + l_n = \frac{r}{2}$ (indem mehrere dieser Koeffizienten auch gleich null sein können).

Für $p = 257$ hat man folgende Zusammenstellung

Summe der Reste	Betrag	Exponent w'	Differenz der Reste	Betrag	Exponent w'
$2 + 1$	3	1	$2 - 1$	1	0
$2^3 + 1$	9	2	$2^3 - 1$	7	5

Da den Exponenten 1, 2, 0, 5 resp. die Perioden $Y_{\frac{9}{16}}$, $Y_{\frac{5}{16}}$, $Y_{\frac{1}{16}}$, $Y_{\frac{11}{16}}$ entsprechen; so ist $l_9 = l_5 = l_1 = l_{11} = 1$, während die übrigen Koeffizienten $= 0$ sind, man hat also

$$Y_{\frac{1}{16}} \cdot Y_{\frac{1}{16}}^{\frac{1}{2}} \cdot Y_{\frac{2}{16}}^{\frac{2}{2}} = Y_{\frac{9}{16}} + Y_{\frac{5}{16}} + Y_{\frac{1}{16}} + Y_{\frac{11}{16}}$$

12) Aus der ersten Periode $Y_{\frac{1}{n}}$ ergiebt sich nach Nr. 5

die zweite $Y_{\frac{2}{n}}$ durch Multiplikation mit $a^{\frac{n}{2}}$

„ dritte $Y_{\frac{3}{n}}$ „ „ „ $a^{\frac{n}{4}}$

„ vierte $Y_{\frac{4}{n}}$ „ „ „ $a^{\frac{n}{2}+\frac{n}{4}}$

„ fünfte $Y_{\frac{5}{n}}$ „ „ „ $a^{\frac{n}{8}}$

u. s. w., d. h. die vier Exponenten w' für die Hälften der zweiten, dritten, vierten etc. Periode ergeben sich aus denen der ersten durch Addition resp. der Werthe $\frac{n}{2}$, $\frac{n}{4}$, $\frac{n}{2}+\frac{n}{4}$, $\frac{n}{8}$ etc., was sofort zur Kenntniss der Perioden führt, aus welchen die Kombinationen

$$Y_{\frac{2}{n}}\cdot\tfrac{1}{2}\quad Y_{\frac{2}{n}}\cdot\tfrac{2}{2},\quad Y_{\frac{3}{n}}\cdot\tfrac{1}{2}\quad Y_{\frac{3}{n}}\cdot\tfrac{2}{2}\text{ etc.}$$

sich zusammensetzen. Für das Beispiel $p = 257$ sind die vor der Tafel Y in Nr. 5 stehenden eingeklammerten Zahlen 8, 4, 12, 2 etc. diejenigen, welche zu den vorstehend gefundenen Werthen von w' zu addiren sind. Danach verzeichnen wir die Exponenten w' in folgender Zusammenstellung, worin wir für einen Exponenten, welcher grösser wird als $n = 16$, dessen Rest nach dem Model 16 setzen: daneben notiren wir sofort die entsprechenden Perioden, aus welchen sich die einzelnen Kombinationen der Halbperioden zusammensetzen.

			Werthe von w'				Werthe der Kombinationen			
für	$Y_{\frac{1}{16}}\cdot\frac{1}{2}$	$Y_{\frac{1}{16}}\cdot\frac{2}{2}$	1	2	0	5	$Y_{\frac{9}{16}}+Y_{\frac{5}{16}}$	$+Y_{\frac{1}{16}}$	$+Y_{\frac{11}{16}}$
„	$Y_{\frac{2}{16}}\cdot\frac{1}{2}$	$Y_{\frac{2}{16}}\cdot\frac{2}{2}$	9	10	8	13	$Y_{\frac{10}{16}}+Y_{\frac{6}{16}}$	$+Y_{\frac{2}{16}}$	$+Y_{\frac{12}{16}}$
„	$Y_{\frac{3}{16}}\cdot\frac{1}{2}$	$Y_{\frac{3}{16}}\cdot\frac{2}{2}$	5	6	4	9	$Y_{\frac{11}{16}}+Y_{\frac{7}{16}}$	$+Y_{\frac{3}{16}}$	$+Y_{\frac{10}{16}}$
„	$Y_{\frac{4}{16}}\cdot\frac{1}{2}$	$Y_{\frac{4}{16}}\cdot\frac{2}{2}$	13	14	12	1	$Y_{\frac{12}{16}}+Y_{\frac{8}{16}}$	$+Y_{\frac{4}{16}}$	$+Y_{\frac{9}{16}}$
„	$Y_{\frac{5}{16}}\cdot\frac{1}{2}$	$Y_{\frac{5}{16}}\cdot\frac{2}{2}$	3	4	2	7	$Y_{\frac{13}{16}}+Y_{\frac{3}{16}}$	$+Y_{\frac{5}{16}}$	$+Y_{\frac{15}{16}}$
„	$Y_{\frac{6}{16}}\cdot\frac{1}{2}$	$Y_{\frac{6}{16}}\cdot\frac{2}{2}$	11	12	10	15	$Y_{\frac{14}{16}}+Y_{\frac{4}{16}}$	$+Y_{\frac{6}{16}}$	$+Y_{\frac{16}{16}}$
„	$Y_{\frac{7}{16}}\cdot\frac{1}{2}$	$Y_{\frac{7}{16}}\cdot\frac{2}{2}$	7	8	6	11	$Y_{\frac{15}{16}}+Y_{\frac{2}{16}}$	$+Y_{\frac{7}{16}}$	$+Y_{\frac{14}{16}}$
„	$Y_{\frac{8}{16}}\cdot\frac{1}{2}$	$Y_{\frac{8}{16}}\cdot\frac{2}{2}$	15	0	14	3	$Y_{\frac{16}{16}}+Y_{\frac{1}{16}}$	$+Y_{\frac{8}{16}}$	$+Y_{\frac{13}{16}}$
„	$Y_{\frac{9}{16}}\cdot\frac{1}{2}$	$Y_{\frac{9}{16}}\cdot\frac{2}{2}$	2	3	1	6	$Y_{\frac{5}{16}}+Y_{\frac{13}{16}}$	$+Y_{\frac{9}{16}}$	$+Y_{\frac{7}{16}}$
„	$Y_{\frac{10}{16}}\cdot\frac{1}{2}$	$Y_{\frac{10}{16}}\cdot\frac{2}{2}$	10	11	9	14	$Y_{\frac{6}{16}}+Y_{\frac{14}{16}}$	$+Y_{\frac{10}{16}}$	$+Y_{\frac{8}{16}}$
„	$Y_{\frac{11}{16}}\cdot\frac{1}{2}$	$Y_{\frac{11}{16}}\cdot\frac{2}{2}$	6	7	5	10	$Y_{\frac{7}{16}}+Y_{\frac{15}{16}}$	$+Y_{\frac{11}{16}}$	$+Y_{\frac{6}{16}}$
„	$Y_{\frac{12}{16}}\cdot\frac{1}{2}$	$Y_{\frac{12}{16}}\cdot\frac{2}{2}$	14	15	13	2	$Y_{\frac{8}{16}}+Y_{\frac{16}{16}}$	$+Y_{\frac{12}{16}}$	$+Y_{\frac{5}{16}}$
„	$Y_{\frac{13}{16}}\cdot\frac{1}{2}$	$Y_{\frac{13}{16}}\cdot\frac{2}{2}$	4	5	3	8	$Y_{\frac{3}{16}}+Y_{\frac{11}{16}}$	$+Y_{\frac{13}{16}}$	$+Y_{\frac{2}{16}}$
„	$Y_{\frac{14}{16}}\cdot\frac{1}{2}$	$Y_{\frac{14}{16}}\cdot\frac{2}{2}$	12	13	11	0	$Y_{\frac{4}{16}}+Y_{\frac{12}{16}}$	$+Y_{\frac{14}{16}}$	$+Y_{\frac{1}{16}}$
„	$Y_{\frac{15}{16}}\cdot\frac{1}{2}$	$Y_{\frac{15}{16}}\cdot\frac{2}{2}$	8	9	7	12	$Y_{\frac{2}{16}}+Y_{\frac{10}{16}}$	$+Y_{\frac{15}{16}}$	$+Y_{\frac{4}{16}}$
„	$Y_{\frac{16}{16}}\cdot\frac{1}{2}$	$Y_{\frac{16}{16}}\cdot\frac{2}{2}$	0	1	15	4	$Y_{\frac{1}{16}}+Y_{\frac{9}{16}}$	$+Y_{\frac{16}{16}}$	$+Y_{\frac{3}{16}}$

13) Um die Halbperioden $Y_{\frac{1}{n}\cdot\frac{1}{2}}$ und $Y_{\frac{1}{n}\cdot\frac{2}{2}}$ resp. in die Viertelperioden $Y_{\frac{1}{n}\cdot\frac{1}{4}}$, $Y_{\frac{1}{n}\cdot\frac{2}{4}}$ und $Y_{\frac{1}{n}\cdot\frac{3}{4}}$, $Y_{\frac{1}{n}\cdot\frac{4}{4}}$ zu zerlegen, sind für die erste Kombination $Y_{\frac{1}{n}\cdot\frac{1}{4}}$ $Y_{\frac{1}{n}\cdot\frac{2}{4}}$ die Zahlen

$$2^{4u+2} \pm 2^{4v} = a^{\alpha}$$

zu betrachten, welche durch Multiplikation mit den $\frac{r}{2}$ Potenzen 2^0, 2^2, $2^4 \ldots 2^{r-2}$ immer volle Halbperioden ergeben. Zu dem Ende sind die $\frac{r}{4}$ Zahlen

$$2^2 \pm 1 \qquad 2^6 \pm 1 \qquad 2^{10} \pm 1 \ldots 2^{\frac{r}{2}-2} \pm 1$$

zu bilden und die Exponenten $w = w' + x\,n$ der ihnen äquivalenten Potenzen a^w zu bestimmen, woraus sich unmittelbar die gesuchten Halbperioden ergeben, wenn man dabei zugleich die Stelle berücksichtigt, welche die zu diesem Exponenten gehörige Zahl a^w selbst einnimmt. Für $p = 257$ hat man

Summe der Reste	Betrag	Exponent w'	Differenz der Reste	Betrag	Exponent w'
$2^2 + 1$	5	7	$2^2 - 1$	3	1

Dem Exponenten 7 entspricht die Periode $Y_{\frac{15}{16}}$ und da die zugehörige Zahl 5 in der zweiten Hälfte dieser Periode steht, die Halbperiode $Y_{\frac{15}{16}\cdot\frac{2}{2}}$. Dem Exponenten 1 entspricht die Periode $Y_{\frac{9}{16}}$ und da die zugehörige Zahl 3 in der ersten Hälfte dieser Periode steht, die Halbperiode $Y_{\frac{9}{16}\cdot\frac{1}{2}}$. Hiernach hat man

$$Y_{\frac{1}{16}\cdot\frac{1}{4}}\ Y_{\frac{1}{16}\cdot\frac{2}{4}} = Y_{\frac{15}{16}\cdot\frac{2}{2}} + Y_{\frac{9}{16}\cdot\frac{1}{2}}$$

Für die zweite Kombination $Y_{\frac{1}{n}\cdot\frac{3}{4}}$ $Y_{\frac{1}{n}\cdot\frac{4}{4}}$ sind die Zahlen

$$2^{4u+3} \pm 2^{4v+1} = 2\,(2^{4u+2} \pm 2^{4v}) = a^{\alpha}$$

zu betrachten, welche durch Multiplikation mit den $\frac{r}{2}$ Potenzen 2^0, 2^2, $2^4 \ldots 2^{r-2}$ volle Halbperioden ergeben. Diese Zahlen sind das Zweifache der vorher betrachteten, sie gehören also denselben Perioden, jedoch nicht denselben, sondern den entgegengesetzten Halbperioden an, weil eine

Multiplikation der Zahlen einer Halbperiode mit 2 gleichbedeutend ist mit der Versetzung dieser Zahlen in die andere Halbperiode. Demnach ist für $p = 257$

$$Y_{\frac{1}{16}\cdot\frac{3}{4}}\, Y_{\frac{1}{16}\cdot\frac{4}{4}} = Y_{\frac{15}{16}\cdot\frac{1}{2}} + Y_{\frac{9}{16}\cdot\frac{2}{2}}$$

14) Aus den Kombinationen der Viertel der ersten Periode ergeben sich die der zweiten, dritten, vierten etc. Periode, wenn man zu den Exponenten der in vorstehender Nummer betrachteten Zahlen die in Nr. 12 bezeichneten Werthe addirt, weil jede folgende Periode aus der vorhergehenden durch Multiplikation mit einer Potenz von a entsteht. Da durch eine solche Multiplikation die Zahlen der Gruppe Y nur in vertikaler Linie sich verrücken, solange der Exponent von a nicht über den Werth $n - 1$ hinaussteigt; so bleibt die Bewegung immer in derselben Hälfte, in welcher sie beginnt, solange der Exponent $w' < n$ bleibt. Sowie jedoch dieser Exponent $\geq n$ wird und nun die nach dem Model n kongruente Zahl $w' - n$ dafür gesetzt wird, springt die betreffende Zahl in die andere Hälfte der Periode über.

Hiernach schreiben wir sofort für $p = 257$, indem sich die beiden Exponenten 7, 1 durch Addition von 8, 4, 12, 2, 10, 6, 14, 1, 9, 5, 13, 3, 11, 7, 15 in 15, 9 — 11, 5 — **3**, 13 — **9**, 3 — **1**, 11 — 13, 7 — **5**, 15 — 8, 2 — **0**, 10 — 12, 6 — **4**, 14 — 10, 4 — **2**, 12 — 14, 8 — **6**, **0** verwandeln und die entgegengesetzte Halbperiode da zu nehmen ist, wo der zugehörige Exponent fett gedruckt ist.

$$Y_{\frac{1}{16}\cdot\frac{1}{4}}\, Y_{\frac{1}{16}\cdot\frac{2}{4}} = Y_{\frac{15}{16}\cdot\frac{2}{2}} + Y_{\frac{9}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{1}{16}\cdot\frac{3}{4}}\, Y_{\frac{1}{16}\cdot\frac{4}{4}} = Y_{\frac{15}{16}\cdot\frac{1}{2}} + Y_{\frac{9}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{2}{16}\cdot\frac{1}{4}}\, Y_{\frac{2}{16}\cdot\frac{2}{4}} = Y_{\frac{16}{16}\cdot\frac{2}{2}} + Y_{\frac{10}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{2}{16}\cdot\frac{3}{4}}\, Y_{\frac{2}{16}\cdot\frac{4}{4}} = Y_{\frac{16}{16}\cdot\frac{1}{2}} + Y_{\frac{10}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{3}{16}\cdot\frac{1}{4}}\, Y_{\frac{3}{16}\cdot\frac{2}{4}} = Y_{\frac{14}{16}\cdot\frac{2}{2}} + Y_{\frac{11}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{3}{16}\cdot\frac{3}{4}}\, Y_{\frac{3}{16}\cdot\frac{4}{4}} = Y_{\frac{14}{16}\cdot\frac{1}{2}} + Y_{\frac{11}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{4}{16}\cdot\frac{1}{4}}\, Y_{\frac{4}{16}\cdot\frac{2}{4}} = Y_{\frac{13}{16}\cdot\frac{1}{2}} + Y_{\frac{12}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{4}{16}\cdot\frac{3}{4}}\, Y_{\frac{4}{16}\cdot\frac{4}{4}} = Y_{\frac{13}{16}\cdot\frac{2}{2}} + Y_{\frac{12}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{5}{16}\cdot\frac{1}{4}}\, Y_{\frac{5}{16}\cdot\frac{2}{4}} = Y_{\frac{10}{16}\cdot\frac{2}{2}} + Y_{\frac{13}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{5}{16}\cdot\frac{3}{4}}\, Y_{\frac{5}{16}\cdot\frac{4}{4}} = Y_{\frac{10}{16}\cdot\frac{1}{2}} + Y_{\frac{13}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{6}{16}\cdot\frac{1}{4}}\, Y_{\frac{6}{16}\cdot\frac{2}{4}} = Y_{\frac{9}{16}\cdot\frac{1}{2}} + Y_{\frac{14}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{6}{16}\cdot\frac{3}{4}}\, Y_{\frac{6}{16}\cdot\frac{4}{4}} = Y_{\frac{9}{16}\cdot\frac{2}{2}} + Y_{\frac{14}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{7}{16}\cdot\frac{1}{4}}\, Y_{\frac{7}{16}\cdot\frac{2}{4}} = Y_{\frac{12}{16}\cdot\frac{2}{2}} + Y_{\frac{15}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{7}{16}\cdot\frac{3}{4}}\, Y_{\frac{7}{16}\cdot\frac{4}{4}} = Y_{\frac{12}{16}\cdot\frac{1}{2}} + Y_{\frac{15}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{8}{16}\cdot\frac{1}{4}}\, Y_{\frac{8}{16}\cdot\frac{2}{4}} = Y_{\frac{11}{16}\cdot\frac{1}{2}} + Y_{\frac{16}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{8}{16}\cdot\frac{3}{4}}\, Y_{\frac{8}{16}\cdot\frac{4}{4}} = Y_{\frac{11}{16}\cdot\frac{2}{2}} + Y_{\frac{16}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{9}{16}\cdot\frac{1}{4}}\, Y_{\frac{9}{16}\cdot\frac{2}{4}} = Y_{\frac{2}{16}\cdot\frac{2}{2}} + Y_{\frac{5}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{9}{16}\cdot\frac{3}{4}}\, Y_{\frac{9}{16}\cdot\frac{4}{4}} = Y_{\frac{2}{16}\cdot\frac{1}{2}} + Y_{\frac{5}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{10}{16}\cdot\frac{1}{4}}\, Y_{\frac{10}{16}\cdot\frac{2}{4}} = Y_{\frac{1}{16}\cdot\frac{1}{2}} + Y_{\frac{6}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{10}{16}\cdot\frac{3}{4}}\, Y_{\frac{10}{16}\cdot\frac{4}{4}} = Y_{\frac{1}{16}\cdot\frac{2}{2}} + Y_{\frac{6}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{11}{16}\cdot\frac{1}{4}}\, Y_{\frac{11}{16}\cdot\frac{2}{4}} = Y_{\frac{4}{16}\cdot\frac{2}{2}} + Y_{\frac{7}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{11}{16}\cdot\frac{3}{4}}\, Y_{\frac{11}{16}\cdot\frac{4}{4}} = Y_{\frac{4}{16}\cdot\frac{1}{2}} + Y_{\frac{7}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{12}{16}\cdot\frac{1}{4}}\,Y_{\frac{12}{16}\cdot\frac{2}{4}} = Y_{\frac{3}{16}\cdot\frac{1}{2}} + Y_{\frac{8}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{12}{16}\cdot\frac{3}{4}}\,Y_{\frac{12}{16}\cdot\frac{4}{4}} = Y_{\frac{3}{16}\cdot\frac{2}{2}} + Y_{\frac{8}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{13}{16}\cdot\frac{1}{4}}\,Y_{\frac{13}{16}\cdot\frac{2}{4}} = Y_{\frac{6}{16}\cdot\frac{2}{2}} + Y_{\frac{3}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{13}{16}\cdot\frac{3}{4}}\,Y_{\frac{13}{16}\cdot\frac{4}{4}} = Y_{\frac{6}{16}\cdot\frac{1}{2}} + Y_{\frac{3}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{14}{16}\cdot\frac{1}{4}}\,Y_{\frac{14}{16}\cdot\frac{2}{4}} = Y_{\frac{5}{16}\cdot\frac{1}{2}} + Y_{\frac{4}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{14}{16}\cdot\frac{3}{4}}\,Y_{\frac{14}{16}\cdot\frac{4}{4}} = Y_{\frac{5}{16}\cdot\frac{2}{2}} + Y_{\frac{4}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{15}{16}\cdot\frac{1}{4}}\,Y_{\frac{15}{16}\cdot\frac{2}{4}} = Y_{\frac{8}{16}\cdot\frac{2}{2}} + Y_{\frac{2}{16}\cdot\frac{1}{2}} \qquad Y_{\frac{15}{16}\cdot\frac{3}{4}}\,Y_{\frac{15}{16}\cdot\frac{4}{4}} = Y_{\frac{8}{16}\cdot\frac{1}{2}} + Y_{\frac{2}{16}\cdot\frac{2}{2}}$$

$$Y_{\frac{16}{16}\cdot\frac{1}{4}}\,Y_{\frac{16}{16}\cdot\frac{2}{4}} = Y_{\frac{7}{16}\cdot\frac{1}{2}} + Y_{\frac{1}{16}\cdot\frac{2}{2}} \qquad Y_{\frac{16}{16}\cdot\frac{3}{4}}\,Y_{\frac{16}{16}\cdot\frac{4}{4}} = Y_{\frac{7}{16}\cdot\frac{2}{2}} + Y_{\frac{1}{16}\cdot\frac{1}{2}}$$

15) Für die erste Kombination $Y_{\frac{1}{n}\cdot\frac{1}{8}}\,Y_{\frac{1}{n}\cdot\frac{3}{8}}$ der Achtelperioden sind die Zahlen

$$2^{8n+4} \pm 2^{8n} = a^{\alpha}$$

zu betrachten, welche durch die Multiplikation mit den $\frac{r}{4}$ Potenzen $2^0, 2^4, 2^8 \ldots 2^{r-4}$ volle Viertelperioden ergeben. Zu dem Ende müssen die $\frac{r}{8}$ Zahlen

$$2^4 \pm 1 \qquad 2^{12} \pm 1 \qquad 2^{20} \pm 1 \ldots 2^{\frac{r}{2}-4} \pm 1$$

gebildet und die Exponenten $w = w' + xn$ der ihnen äquivalenten Potenzen a^w bestimmt werden.

16) Wenn $r = 2^s$; so führt die s-te Halbirung auf die einzelnen Reste $Y_{\frac{1}{n}\cdot\frac{1}{r}}$. In diesem Falle sind die Zahlen von der Form

$$2^{rn+\frac{r}{2}} \pm 2^{rn} = a^{\alpha}$$

zu betrachten. Da keine höhere, als die r-te Potenz von 2 in Betracht kömmt; so reduzirt sich die Reihe der zu bildenden Zahlen auf die zwei Zahlen $2^{\frac{r}{2}} \pm 1$. Dieselben gehören einunderselben Theilperiode an, sodass für beide der Exponent w' denselben Werth hat: denn da $2^{\frac{r}{2}}(2^{\frac{r}{2}} - 1) = 2^r - 2^{\frac{r}{2}} = p - 1 - 2^{\frac{r}{2}} \equiv -1 - 2^{\frac{r}{2}}$, also äquivalent $2^{\frac{r}{2}} + 1$ ist; so stehen die beiden Zahlen $2^{\frac{r}{2}} + 1$ und $2^{\frac{r}{2}} - 1$ in derselben Periode.

Für $p = 257$, $r = 8$ hat man die Zahlen $2^4 \pm 1$ zu bilden, welche folgende Werthe liefern.

Summe der Reste	Betrag	Exponent w'	Summe der Differenzen	Betrag	Exponent w'
$2^4 + 1$	17	8	$2^4 - 1$	15	8

Die beiden Zahlen 17 und 15 gehören derselben Viertelperiode vom Exponenten 8 und zwar der dritten an, d. h. man hat, da der Exponent 8 die zweite Periode $Y_{\frac{2}{16}}$ anzeigt,

$$Y_{\frac{1}{16}} \cdot \tfrac{1}{8}\; Y_{\frac{1}{16}} \cdot \tfrac{2}{8} = Y_{\frac{2}{16}} \cdot \tfrac{3}{4}$$

Die Zahlen der zweiten Achtelperiode sind das $2^2 = 4$-fache der Zahlen der ersten. Statt $2^1 \pm 1$ kommen daher jetzt die Zahlen $2^2(2^1 \pm 1)$ in Betracht, welche in derselben zweiten Periode wie jene, jedoch im vierten Viertel liegen, sodass man

$$Y_{\frac{1}{16}} \cdot \tfrac{3}{8}\; Y_{\frac{1}{16}} \cdot \tfrac{4}{8} = Y_{\frac{2}{16}} \cdot \tfrac{4}{4}$$

hat. Für die dritte Achtelperiode handelt es sich um die Zahlen $2(2^1 \pm 1)$, welche ebenfalls in derselben zweiten Periode, jedoch in dem zweiten Viertel liegen, sodass man

$$Y_{\frac{1}{16}} \cdot \tfrac{5}{8}\; Y_{\frac{1}{16}} \cdot \tfrac{6}{8} = Y_{\frac{2}{16}} \cdot \tfrac{2}{4}$$

hat. Für die vierte Achtelperiode handelt es sich um die Zahlen $2^3(2^1 \pm 1)$, welche in derselben zweiten Periode, jedoch im ersten Viertel liegen, wonach

$$Y_{\frac{1}{16}} \cdot \tfrac{7}{8}\; Y_{\frac{1}{16}} \cdot \tfrac{8}{8} = Y_{\frac{2}{16}} \cdot \tfrac{1}{4}$$

ist. Wie die erste Periode so zerlegt sich die zweite, wenn man beachtet, dass die Zahlen dieser Periode aus denen der ersten durch Multiplikation mit a^8 hervorgehen, dass sich also der Exponent $w' = 8$ auf $8 + 8 = 16$ erhöht oder $= 0$ wird. Hierdurch wird

$$Y_{\frac{2}{16}} \cdot \tfrac{1}{8}\; Y_{\frac{2}{16}} \cdot \tfrac{2}{8} = Y_{\frac{1}{16}} \cdot \tfrac{1}{4} \qquad Y_{\frac{2}{16}} \cdot \tfrac{3}{8}\; Y_{\frac{2}{16}} \cdot \tfrac{4}{6} = Y_{\frac{1}{16}} \cdot \tfrac{2}{4}$$

$$Y_{\frac{2}{16}} \cdot \tfrac{5}{8}\; Y_{\frac{2}{16}} \cdot \tfrac{6}{8} = Y_{\frac{1}{16}} \cdot \tfrac{3}{4} \qquad Y_{\frac{2}{16}} \cdot \tfrac{7}{8}\; Y_{\frac{1}{16}} \cdot \tfrac{8}{8} = Y_{\frac{1}{16}} \cdot \tfrac{4}{4}$$

Die dritte Periode geht aus der ersten durch Multiplikation mit a^4 hervor, der Exponent $w' = 8$ wird also $8 + 4 = 12$ und

$$Y_{\frac{3}{16}} \cdot \tfrac{1}{8}\; Y_{\frac{3}{16}} \cdot \tfrac{2}{8} = Y_{\frac{4}{16}} \cdot \tfrac{3}{4} \qquad Y_{\frac{3}{16}} \cdot \tfrac{3}{8}\; Y_{\frac{3}{16}} \cdot \tfrac{4}{8} = Y_{\frac{4}{16}} \cdot \tfrac{4}{4}$$

$$Y_{\frac{3}{16}} \cdot \tfrac{5}{8}\; Y_{\frac{3}{16}} \cdot \tfrac{6}{8} = Y_{\frac{4}{16}} \cdot \tfrac{2}{4} \qquad Y_{\frac{3}{16}} \cdot \tfrac{7}{8}\; Y_{\frac{3}{16}} \cdot \tfrac{8}{8} = Y_{\frac{4}{16}} \cdot \tfrac{1}{4}$$

Die vierte Periode erfolgt aus der ersten durch Multiplikation mit 12, der Exponent $w' = 8$ verwandelt sich also wegen $8 + 12 = 20$ in 4 und man hat

$$Y_{\frac{4}{16}} \cdot \tfrac{1}{8}\; Y_{\frac{4}{16}} \cdot \tfrac{2}{8} = Y_{\frac{3}{16}} \cdot \tfrac{1}{4} \qquad Y_{\frac{4}{16}} \cdot \tfrac{3}{8}\; Y_{\frac{4}{16}} \cdot \tfrac{4}{8} = Y_{\frac{3}{16}} \cdot \tfrac{2}{4}$$

$$Y_{\frac{4}{16}} \cdot \tfrac{5}{8}\; Y_{\frac{4}{16}} \cdot \tfrac{6}{8} = Y_{\frac{3}{16}} \cdot \tfrac{3}{4} \qquad Y_{\frac{4}{16}} \cdot \tfrac{7}{8}\; Y_{\frac{4}{16}} \cdot \tfrac{8}{8} = Y_{\frac{3}{16}} \cdot \tfrac{4}{4}$$

Wir stellen die Nummern der Perioden und deren Viertel, welche den Kombinationen des ersten und zweiten, des dritten und vierten, des fünften und sechsten, des siebenten und achten Achtels der 16 aufeinander folgenden Perioden gleich sind, in folgende Tabelle zusammen.

Periode der Achtel	Periode der Viertel	Nummern der Viertel			
1	2	3	4	2	1
2	1	1	2	3	4
3	4	3	4	2	1
4	3	1	2	3	4
5	6	3	4	2	1
6	5	1	2	3	4
7	8	3	4	2	1
8	7	1	2	3	4
9	10	3	4	2	1
10	9	1	2	3	4
11	12	3	4	2	1
12	11	1	2	3	4
13	14	3	4	2	1
14	13	1	2	3	4
15	16	3	4	2	1
16	15	1	2	3	4

17) Statt die Gruppe Y erst horizontal und dann vertikal zu zerlegen, kann man auch erst die vertikale und dann die horizontale Zerlegung vornehmen. Diess hat eine Vertauschung der Koeffizienten k und l ohne Veränderung ihrer Werthe zur Folge.

Man könnte die Frage aufwerfen, ob ein Wechsel der primitiven Wurzel a eine Änderung der Werthe dieser Koeffizienten k und l herbeiführen könne. Diese Frage ist aus folgenden Gründen zu verneinen.

Alle möglichen primitiven Wurzeln $< \frac{1}{2}(p-1)$ bilden die untere Hälfte $Y_{\frac{2}{2}}$ der Gruppe Y in Nr. 5. Nimmt man statt der Wurzel a irgend eine Zahl a_1 derselben Periode oder Horizontalreihe; so unterscheidet sich dieselbe von a nur durch einen Faktor, welcher eine Potenz von 2 ist. Demzufolge unterscheiden sich auch die Potenzen von a_1 von den gleich hohen Potenzen von a nur durch solche Faktoren und demzufolge nimmt die erste, zweite, dritte etc. Horizontalreihe der neuen Gruppe ganz dieselben Reste auf wie resp. die erste, zweite, dritte etc. Horizontalreihe der alten Gruppe. Ausserdem ist klar, dass so, wie sich die Reste der einen Horizontalreihe verstellen, auch die Reste der übrigen Horizontalreihen sich verstellen, und dass Diess auch hinsichtlich der ersten Horizontalreihe gilt, wenn man alle Reste derselben zyklisch so weit vorschiebt, dass sich der Rest 1 über die frühere Wurzel a stellt, sodass in der neuen Gruppe auch die vertikalen Reihen dieselben Zahlen und Zahlenfolgen haben, wie in der alten, und überhaupt nur eine Verstellung der vertikalen Reihen stattfindet, welche jedoch durch die An-

ordnung der Gruppe nach Nr. 5 vollständig ausgeglichen werden kann, indem man alle Vertikalreihen zyklisch so weit verschiebt, dass der Rest 1 wieder der erste wird.

Vertauscht man die Wurzel a_1 mit einer Zahl a_2 aus derselben Vertikalreihe; so hat Diess, weil sich a_2 von a_1 durch eine Potenz von a unterscheidet, eine Verrückung der Horizontalreihen zur Folge, wobei die Reihenfolge in jeder Horizontalreihe eine Änderung erleidet. Durch die Anordnung der Gruppe nach Nr. 5 wird aber bewirkt, dass die erste Horizontalreihe dieselben Zahlen in derselben Reihenfolge wie in der ursprünglichen Gruppe enthält.

Aus allem Diesen geht hervor, dass wegen der Konstanz der horizontalen Perioden (welche nur ihre Stellung und die Reihenfolge ihrer Glieder ändern, die Koeffizienten k ihre Werthe behalten, und dass wegen der Identität der ersten Periode in der geordneten alten und neuen Gruppe auch die Koeffizienten l unveränderlich sind.

Es leuchtet auch ein, dass man bei jeder Halbirung der zuletzt gebildeten Gruppen die beiden Hälften aller einzelnen Gruppen mit einander vertauschen kann (ein Resultat, welches sich durch den Wechsel der primitiven Wurzel hervorbringen lässt).

18) Die Formeln für die Kombinationen der Hälften, der Viertel, der Achtel u. s. w. lassen sich dadurch vereinfachen, dass man auf der rechten Seite erst so viel Ganze, dann so viel Halbe, dann so viel Viertel u. s. w., als die Koeffizienten k oder l zulassen, absondert. Hierdurch verwandelt sich z. B. die für $p = 257$ gültige Formel

$$Y_{\frac{1}{8}}\, Y_{\frac{2}{8}} = 2\, Y_{\frac{1}{4}} + 4\, Y_{\frac{2}{4}} + 5\, Y_{\frac{3}{4}} + 5\, Y_{\frac{4}{4}}$$

in

$$Y_{\frac{1}{8}}\, Y_{\frac{2}{8}} = 2\, Y + 3\, Y_{\frac{2}{2}} + 2\, Y_{\frac{2}{4}}$$

§. 2. Auflösung der Gleichung $x^p - 1 = 0$.

Die vorstehenden Sätze liefern die Summe und das Produkt zweier Theilgruppen als einen ganzen rationalen Ausdruck der nächst höheren Gruppen in der Form

$$Y_\alpha + Y_\beta = A \qquad Y_\alpha \,.\, Y_\beta = B$$

Diese Theilgruppen sind also die Wurzeln der quadratischen Gleichung

$$Y^2 - A\,Y + B = 0$$

Die höchste Gruppe ist die Gesammtgruppe $Y = -1$. Von dieser ausgehend, ergeben sich also die allmählich immer niedriger werdenden Theilgruppen bis zu den niedrigsten, welche die einfachen Glieder X der Gesammtgruppe sind. Für ein jedes solches Glied hat man aber nach Gl. (3)

$$X_\varrho = x^\varrho + x^{-\varrho} = C$$

und hieraus folgen zwei Wurzeln der Gleichung $x^p - 1 = 0$ mittelst der quadratischen Gleichung

$$(x^\varrho)^2 - C x^\varrho + 1 = 0$$

Von diesen beiden Wurzeln ist die eine $x = e^{\frac{2\varrho\pi}{p} i}$ und die andere $x = e^{\frac{-2\varrho\pi}{p} i}$, die Grösse X_ϱ oder die Summe dieser beiden Wurzeln hat also den reellen Werth

$$X_\varrho = 2 \cos \frac{2\varrho\pi}{p}$$

Für die ersten Hälften der Gesammtgruppe hat man

$$Y_{\frac{1}{2}} + Y_{\frac{2}{2}} = -1 \qquad Y_{\frac{1}{2}} Y_{\frac{2}{2}} = -2^{r-2}$$

also, da $2^r + 1 = p$ ist

$$Y_{\frac{1}{2}} = -\frac{1}{2} + \frac{1}{2}\sqrt{p} \qquad Y_{\frac{2}{2}} = -\frac{1}{2} - \frac{1}{2}\sqrt{p}$$

Für die Viertel der Gesammtgruppe ist

$$Y_{\frac{1}{4}} + Y_{\frac{2}{4}} = -\frac{1}{2} + \frac{1}{2}\sqrt{p}$$

$$Y_{\frac{1}{4}} Y_{\frac{2}{4}} = -2^{r-4} + \frac{1}{2}(k_2 - k_3)\sqrt{p}$$

u. s. f.

Für eine Primzahl p von der Form $2^r + 1$ sind hiernach von Anfang bis zu Ende nur quadratische Gleichungen aufzulösen, woraus die Konstruirbarkeit der betreffenden regelmässigen Vielecke mit Kreis und gerader Linie hervorgeht. Die Zweiwerthigkeit der Wurzel einer quadratischen Gleichung findet ihren Ausdruck durch die Zweiwerthigkeit des Quadratwurzelzeichens in dem allgemeinen Ausdrucke der Wurzel. Dieses Zeichen muss also einmal positiv und einmal negativ genommen werden, um beide Wurzeln zu erhalten. Nun handelt es sich aber bei der Halbirung der Hälften, der Viertel, der Achtel u. s. w. immer um ein System von mehreren, nämlich resp. von 2, 4, 8 u. s. w. quadratischen Gleichungen, welche die einzelnen aliquoten Theile der Grundtafel ergeben, und wir heben hervor, dass die fraglichen Quadratwurzeln in den Gleichungen einunddesselben Systems immer mit dem einen Zeichen für die oberen oder vorderen und mit dem entgegengesetzten Zeichen für die unteren oder hinteren Hälften zu nehmen sind, dass aber in jedem einzelnen Systeme für das erstere Zeichen nach Belieben das positive oder das negative genommen werden kann. Die durch solche Zeichenwechsel herbeigeführten Verstellungen der Reste der Grundtafel entsprechen den durch den Wechsel der primitiven Wurzel bedingten Veränderungen.

§. 3. Konstruktion des Polygons von p Seiten.

1) Wenn man es nicht auf die algebraische Berechnung der Wurzel $x^p - 1 = 0$, sondern auf die geometrische Konstruktion des regelmässigen Vieleckes von p Seiten abgesehen hat, thut man wohl, die

quadratischen Gleichungen gar nicht aufzulösen, sondern die Linien, welche den Bedingungen

$$y_1 + y_2 = a \qquad y_1 y_2 = b$$

entsprechen, direkt darzustellen. Zu dem Ende macht man in Fig. 1 auf der Abszissenaxe OB links von O $OE = 1$ und rechts von O $OB = b$, beschreibt über EB den Halbkreis EDB, welcher die Ordinatenaxe in D schneidet, sodass OD die mittlere geometrische Proportionale zwischen 1 und b oder der absoluten Länge nach $OD^2 = b$ ist, zieht DA parallel zur Abszissenaxe, macht $DA = a$, beschreibt über DA als Durchmesser den Kreis $DY_1 Y_2 AZ_2$, welcher die Axe in Y_1 und Y_2 schneidet, und zieht von O durch den Mittelpunkt C dieses Kreises die Linie $OZ_1 Z_2$, welche den Kreis in Z_1 und Z_2 schneidet.

Es sind vier Fälle zu unterscheiden: Ist b positiv und a positiv; so ist $OY_1 = y_1$ und $OY_2 = y_2$. Ist b positiv und a negativ; so ist $-OY_1 = y_1$ und $-OY_2 = y_2$ (Man kann in diesem Falle die Linie $DA = a$ gleich links von D legen, um sofort y_1 und y_2 in der negativen Lage zu erhalten). Ist b negativ und a positiv; so ist $-OZ_1 = y_1$ und $OZ_2 = y_2$. Ist b negativ und a negativ; so ist $OZ_1 = y_1$ und $-OZ_2 = y_2$.

Nachdem durch diese Konstruktion die Längen der obigen beiden Hälften gefunden sind, ergeben sich die Werthe von a und b, welche zur Konstruktion von je zwei Vierteln erforderlich sind, durch einfache Zusammensetzung aus positiven und negativen ganzen Vielfachen der gefundenen Hälften; man gelangt also durch zwei der vorstehenden gleiche Konstruktionen zur Kenntniss der vier Viertel, sodann durch vier ähnliche Konstruktionen zur Kenntniss der acht Achtel u. s. f., bis sich endlich die $\frac{p-1}{2}$ Werthe von X ergeben.

Aus einem Werthe von X_ϱ ergeben sich die Werthe der beiden Wurzeln x^ϱ und $x^{-\varrho}$ ebenfalls sehr leicht ohne Auflösung der Gleichung $x^\varrho + x^{-\varrho} = X_\varrho$. Errichtet man nämlich in Fig. 2 im Endpunkte D des für X gefundenen Werthes OD das Perpendikel CDB und beschreibt um O mit dem Radius $OA = 2$ einen Kreis, welcher das Perpendikel in B und C schneidet; so ist sowohl nach Länge, als auch nach Richtung $OB = 2x^\varrho$ und $OC = 2x^{-\varrho}$ oder AOB ist der Zentrumswinkel $\frac{2\pi}{p}$ des p-ecks, folglich AB und AC eine Seite dieses Polygons in dem Kreise vom Radius 2.

Hat man alle X, die positiven von O gegen A hin, die negativen von O in entgegengesetzter Richtung aufgetragen und alle Perpendikel DB errichtet; so liefern die Durchschnitte derselben mit der Kreislinie CAB alle Endpunkte des p-ecks oder das vollständige Polygon.

Wir bemerken noch, dass $\varrho = 1$ das grösste positive X in dem Ausdrucke $X_1 = 2\cos\frac{2\pi}{p}$, nämlich die doppelte Länge der Abszisse des Endpunktes der ersten Seite des Polygons (im Kreise vom Radius 1) liefert, während $\varrho = \frac{p-1}{2}$, also für $p = 257$ der Werth $\varrho = 128$

das grösste negative X, welches zugleich den absolut grössten numerischen Werth von allen X hat, in dem Ausdrucke

$$X = 2 \cos \frac{p-1}{p} \pi = 2 \cos \left(1 - \frac{1}{p}\right) \pi = - \cos \frac{\pi}{p}$$

also den doppelten Abstand einer Polygonseite vom Mittelpunkte (im Kreise vom Radius 1) darstellt.

Wir wollen diese Konstruktion am regelmässigen Dreieck, Fünfeck und Siebzehneck ausführen.

2) Das Dreieck. Für $p = 2 + 1 = 3$ besteht die ganze Gruppe Y aus der einzigen Zahl 1. Dieselbe enthält die Auflösung für die einzige in Betracht kommende Grösse $X_1 = Y = -1$ und es handelt sich um die einzige Gleichung

$$x^1 + x^{-1} = 1$$

Macht man hiernach in Fig. 3 $OD = -1$ und beschreibt mit dem Radius $OA = 2$ einen Kreis; so schneidet derselbe das in D errichtete Perpendikel in den beiden Punkten B und C, welche mit A das gleichseitige Dreieck ABC bilden.

3) Das Fünfeck. Für $p = 2^2 + 1 = 5$ besteht die Gruppe Y aus der einzigen zweigliedrigen Periode 1, 2; es handelt sich also um eine einzige Halbirung einer Periode nach §. 1 Nr. 11. Die Zahlen 2 ± 1, $2^3 \pm 1$ etc. reduziren sich auf die beiden Zahlen $2 + 1$ und $2 - 1$, wovon die erste $= 3$ äquivalent 2 und die zweite $= 1$ ist, beide aber dem Exponenten $w' = 0$ angehören oder der einen und ersten Periode Y entsprechen. Hiernach hat man

$$Y_{\frac{1}{2}} + Y_{\frac{2}{2}} = Y = -1$$

$$Y_{\frac{1}{2}} \cdot Y_{\frac{2}{2}} = Y = -1$$

Die algebraische Auflösung, welche in dem Ausdrucke für $Y_{\frac{1}{2}}$ die Abszisse des Endpunktes der ersten Seite und in dem Ausdrucke für $Y_{\frac{2}{2}}$ den Abstand der Seite des Fünfeckes vom Mittelpunkte im Kreise vom Radius 2 unmittelbar darstellt, ist

$$Y_{\frac{1}{2}} = X_1 = -\frac{1}{2} + \frac{1}{2}\sqrt{5}$$

$$Y_{\frac{2}{2}} = X_2 = -\frac{1}{2} - \frac{1}{2}\sqrt{5}$$

und demnach

$$x^1 \text{ und } x^{-1} = -\frac{1}{4} + \frac{1}{4}\sqrt{5} \pm \sqrt{-\frac{5}{8} - \frac{1}{8}\sqrt{5}}$$

$$x^2 \text{ und } x^{-2} = -\frac{1}{4} + \frac{1}{4}\sqrt{5} \pm \sqrt{-\frac{5}{8} + \frac{1}{8}\sqrt{5}}$$

Die geometrische Konstruktion vollführen wir nicht nach den letzten Ausdrücken, sondern unmittelbar nach den Bedingungsgleichungen folgendermaassen. In Fig. 4 machen wir $OE = 1$, $OB = 1$, beschreiben über EB den Halbkreis, welcher die Ordinatenaxe in D schneidet, ziehen DA parallel zu OB, beschreiben über $DA = 1$ den Kreis $DFAG$, ziehen von O durch den Mittelpunkt C die Linie OC, welche den Kreis in F und G schneidet; alsdann ist $OF = X_1$ und $-OG = X_2$. Nehmen wir also $OF_1 = OF$ und $OG_1 = OG$, errichten in F_1 und G_1 Perpendikel, so schneidet ein mit dem Radius $OH = 2$ beschriebener Kreis diese Perpendikel in den Punkten J, K, L, M, welche mit H das regelmässige Fünfeck $HJKLM$ in dem Kreise vom Radius 2 bilden.

4) Das Siebzehneck. Für $p = 2^4 + 1 = 17$ erhält man zwei Perioden, welche folgende geordnete Gruppe bilden.

	(0.2)	(2.2)	(3.2)	(1.2)
	2^0	2^2	2^1	2^3
(0)	1	4	2	8
(1)	3	5	6	7

Für die Hälften der Gruppe hat man nach §. 1 Nr. 6

$$Y_{\frac{1}{2}} + Y_{\frac{2}{2}} = Y = -1$$

$$Y_{\frac{1}{2}}\, Y_{\frac{2}{2}} = 4Y = -4$$

Hierdurch sind die beiden Perioden bestimmt. Für die Halbperioden kommen nach Nr. 11 die Zahlen

	Exp. w'		Exp. w'
$2 + 1 = 3$	1	$2 - 1 = 1$	0

in Betracht. Den Exponenten 1, 0 entsprechen resp. die Perioden $Y_{\frac{2}{2}}$ und $Y_{\frac{1}{2}}$, man hat also für die Hälften der ersten Periode

$$Y_{\frac{1}{2}\cdot\frac{1}{2}} + Y_{\frac{1}{2}\cdot\frac{2}{2}} = Y_{\frac{1}{2}}$$

$$Y_{\frac{1}{2}\cdot\frac{1}{2}} \cdot Y_{\frac{1}{2}\cdot\frac{2}{2}} = Y_{\frac{2}{2}} + Y_{\frac{1}{2}} = Y = -1$$

Die Exponenten w' für die Hälften der zweiten Periode ergeben sich aus denen der ersten durch Hinzufügung des Werthes $\frac{n}{2} = \frac{2}{2} = 1$, dieselben sind mithin resp. 0, 1 und entsprechen den Perioden $Y_{\frac{1}{2}}$ und $Y_{\frac{2}{2}}$, sodass man hat

$$Y_{\frac{2}{2}\cdot\frac{1}{2}} + Y_{\frac{2}{2}\cdot\frac{2}{2}} = Y_{\frac{2}{2}}$$

$$Y_{\frac{2}{2}\cdot\frac{1}{2}} \cdot Y_{\frac{2}{2}\cdot\frac{2}{2}} = Y_{\frac{1}{2}} + Y_{\frac{2}{2}} = Y = -1$$

Für die Viertelperioden kommen nach Nr. 13 die Zahlen

$$2^2 + 1 = 5 \qquad \overset{\text{Exp. } w'}{1} \qquad 2^2 - 1 = 3 \qquad \overset{\text{Exp. } w'}{1}$$

in Betracht. Dem Exponenten 1 entspricht die Periode $Y_{\frac{2}{2}}$ und da sowohl die Zahl 5, als auch die Zahl 3 der ersten Hälfte $Y_{\frac{2}{2}\cdot\frac{1}{2}}$ angehört; so ist für die ersten beiden Viertel der ersten Periode

$$Y_{\frac{1}{2}\cdot\frac{1}{4}} + Y_{\frac{1}{2}\cdot\frac{2}{4}} = Y_{\frac{1}{2}\cdot\frac{1}{2}}$$
$$Y_{\frac{1}{2}\cdot\frac{1}{4}} \cdot Y_{\frac{1}{2}\cdot\frac{2}{4}} = Y_{\frac{2}{2}\cdot\frac{1}{2}}$$

Für die anderen beiden Viertel der ersten Periode ist, indem dafür die Zahlen 5 und 3 sich in 10 und 6 oder in 7 und 6 verwandlen, denen ebenfalls die Exponenten 1 und 1 angehören, die jetzt jedoch die zweite Hälfte der Periode anzeigen,

$$Y_{\frac{1}{2}\cdot\frac{3}{4}} + Y_{\frac{1}{2}\cdot\frac{4}{4}} = Y_{\frac{1}{2}\cdot\frac{2}{2}}$$
$$Y_{\frac{1}{2}\cdot\frac{3}{4}} \cdot Y_{\frac{1}{2}\cdot\frac{4}{4}} = Y_{\frac{2}{2}\cdot\frac{2}{2}}$$

Die Viertel der zweiten Periode ergeben sich nach Nr. 14, wenn man zu den Exponenten w' den Werth $\frac{n}{2} = 1$ addirt und das Überspringen in die andere Periodenhälfte beachtet. Hierdurch erhält man für die ersten beiden Viertel

$$Y_{\frac{2}{2}\cdot\frac{1}{4}} + Y_{\frac{2}{2}\cdot\frac{2}{4}} = Y_{\frac{2}{2}\cdot\frac{1}{2}}$$
$$Y_{\frac{2}{2}\cdot\frac{1}{4}} \cdot Y_{\frac{2}{2}\cdot\frac{2}{4}} = Y_{\frac{1}{2}\cdot\frac{2}{2}}$$

und für die letzten beiden Viertel

$$Y_{\frac{2}{2}\cdot\frac{3}{4}} + Y_{\frac{2}{2}\cdot\frac{4}{4}} = Y_{\frac{2}{2}\cdot\frac{2}{2}}$$
$$Y_{\frac{2}{2}\cdot\frac{3}{4}} \cdot Y_{\frac{2}{2}\cdot\frac{4}{4}} = Y_{\frac{1}{2}\cdot\frac{1}{2}}$$

Eine Auflösung dieser Gleichungen ergiebt, wenn man beachtet, dass

$$(-1 + \sqrt{17}) \sqrt{34 - 2\sqrt{17}}$$
$$= (1 + \sqrt{17}) \sqrt{34 - 2\sqrt{17}} - 2 \sqrt{34 - 2\sqrt{17}}$$
$$= 4 \sqrt{34 + 2\sqrt{17}} - 2 \sqrt{34 - 2\sqrt{17}}$$

und dass

$$(1+\sqrt{17})\sqrt{34+2\sqrt{17}}$$
$$= (-1+\sqrt{17})\sqrt{34+2\sqrt{17}} + 2\sqrt{34+2\sqrt{17}}$$
$$= 4\sqrt{34-2\sqrt{17}} + 2\sqrt{34+2\sqrt{17}}$$

ist, alle 8 Werthe der Grössen X in der einen Formel

$$X = -\frac{1}{8} + (-1)^{\alpha}\frac{1}{8}\sqrt{17} + (-1)^{\beta}\frac{1}{8}\sqrt{34+(-1)^{\alpha+1}\,2\sqrt{17}}$$
$$+(-1)^{\gamma}\frac{1}{4}\sqrt{\left\{17+(-1)^{\alpha}3\sqrt{17}+(-1)^{\beta+1}\sqrt{34+(-1)^{\alpha+1}\,2\sqrt{17}}\right.}$$
$$\left.+\,(-1)^{\alpha+\beta+1}\,2\sqrt{34+(-1)^{\alpha}\,2\sqrt{17}}\right\}$$

Hierin kann man den drei Exponenten α, β, γ beliebige ganze Werthe geben.

Die 8 Werthe von X unterscheiden sich nur durch die Zweideutigkeit der in diesem Ausdrucke enthaltenen Quadratwurzeln. Der grösste positive Werth für $\frac{1}{2}X = \cos\frac{2\pi}{17}$ ist

$$\cos\frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34-2\sqrt{17}}$$
$$+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

welchen Gauss in den Disq. arithm. art. 365 angiebt. Der grösste negative Werth, welcher den Abstand der Seite des Siebzehnecks vom Mittelpunkte im Kreise vom Radius 1 anzeigt, hat den absoluten Werth

$$\cos\frac{16\pi}{17} = \frac{1}{16} - \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34+2\sqrt{17}}$$
$$+\frac{1}{8}\sqrt{17+3\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{34+2\sqrt{17}}}$$

Die geometrische Konstruktion des Siebzehneckes nach der obigen Regel ist in Fig. 5 dargestellt. Da für die erste Konstruktion die mittlere geometrische Proportionale zwischen 1 und 4 gleich 2 und für die zweite und dritte Konstruktion die mittlere geometrische Proportionale zwischen

1 und 1 gleich 1 ist; so haben wir der Kürze halber sofort über der Abszissenlinie, in welcher $OE = 1$ ist, die Ordinate $Oa = 2$ und $Ob = 1$ verzeichnet, und für die erste Konstruktion über $aa' = 1$ als Durchmesser den Kreis beschrieben, welcher $O1 = Y_{\frac{1}{2}}$ und $O2 = -Y_{\frac{2}{2}}$ ergiebt. Hierauf ist über $bb' = O1$ der Kreis beschrieben, welcher $O3 = Y_{\frac{1}{2}\,\frac{1}{2}}$ und $O4 = 4 - Y_{\frac{1}{2}\,\frac{2}{2}}$ ergiebt, ferner über $bb'' = O2$ der Kreis, welcher $O5 = Y_{\frac{2}{2}\,\frac{1}{2}}$ und $O6 = Y_{\frac{2}{2}\,\frac{2}{2}}$ liefert. Darauf ist zu 1 und $O5$ die mittlere Proportionale Oc konstruirt und über $cc' = O3$ der Halbkreis beschrieben, welcher $O7 = Y_{\frac{1}{2}\,\frac{1}{4}}$ und und $O8 = Y_{\frac{1}{2}\,\frac{2}{4}}$ ergiebt. Alsdann ist zu 1 und $O6$ die mittlere Proportionale Od konstruirt und über $dd' = O4$ der Kreis beschrieben, welcher $O9 = Y_{\frac{1}{2}\,\frac{3}{4}}$ und $O10 = -Y_{\frac{1}{2}\,\frac{4}{4}}$ liefert. Hierauf ist zu 1 und $O4$ die mittlere Proportionale Oe konstruirt und über $ee' = O5$ der Kreis beschrieben, welcher $O11 = Y_{\frac{2}{2}\,\frac{1}{4}}$ und $O12 = -Y_{\frac{2}{2}\,\frac{2}{4}}$ liefert. Endlich ist zu 1 und $O3$ die mittlere Proportionale Of konstruirt und über $ff' = O6$ der Halbkreis beschrieben, welcher $O13 = -Y_{\frac{2}{2}\,\frac{3}{4}}$ und $O14 = -Y_{\frac{2}{2}\,\frac{4}{4}}$ ergiebt.

Die Zahlen 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 weisen also resp. auf die Grössen $Y_{\frac{1}{2}}$, $Y_{\frac{2}{2}}$, $Y_{\frac{1}{2}\,\frac{1}{2}}$, $Y_{\frac{1}{2}\,\frac{2}{2}}$, $Y_{\frac{2}{2}\,\frac{1}{2}}$, $Y_{\frac{2}{2}\,\frac{2}{2}}$, $Y_{\frac{1}{2}\,\frac{1}{4}}$, $Y_{\frac{1}{2}\,\frac{2}{4}}$, $Y_{\frac{1}{2}\,\frac{3}{4}}$, $Y_{\frac{1}{2}\,\frac{4}{4}}$, $Y_{\frac{2}{2}\,\frac{1}{4}}$, $Y_{\frac{2}{2}\,\frac{2}{4}}$, $Y_{\frac{2}{2}\,\frac{3}{4}}$, $Y_{\frac{2}{2}\,\frac{4}{4}}$ hin. Die den 7 Zahlen 1, 3, 5, 7, 8, 9, 11 entsprechenden Grössen sind positiv, die den 7 Zahlen 2, 4, 6, 10, 12, 13, 14 entsprechenden Grössen sind negativ. Die 8 Zahlen 7, 8, 9, 10, 11, 12, 13, 14 bestimmen die 8 Werthe von X oder die Abszissen der Ecken des Siebzehneckes im Kreise vom Radius $OA = OB = 2$. Die den 4 Zahlen 7, 8, 9, 11 entsprechenden Abszissen sind positiv, die den 4 Zahlen 10, 12, 13, 14 entsprechenden sind negativ.

Die in den Punkten 7, 8, 9, 10, 11, 12, 13, 14 errichteten Ordinaten führen in die 16 Ecken des Siebzehneckes, dessen 17. Ecke der Punkt B ist. Man erhält also durch diese einfache Konstruktion nicht nur eine einzelne Seite, sondern das ganze Siebzehneck und alle seine wesentlichen Abmessungen.

Wollte man nur die eine an B liegende Seite, also die Abszisse $O7$ darstellen; so bedürfte es nur der ersten vier Konstruktionen, und wollte man nur den Abstand der Seite vom Mittelpunkte, also die Abszisse $O10$ verzeichnen; so bedürfte es nur der ersten drei und der fünften Konstruktion.

5) Das Zweihundertsiebenundfunfzigeck. Für $p = 2^8 + 1 = 257$ erhält man die schon im §. 1 gebildeten Perioden. Die Rechnung beginnt so: Nach Nr. 6 ist

$$Y_{\frac{1}{2}} + Y_{\frac{2}{2}} = -1$$

$$Y_{\frac{1}{2}}\, Y_{\frac{2}{2}} = -2^{r-2} = -64$$

also

$$Y_{\frac{1}{2}} = -\frac{1}{2} + \frac{1}{2}\sqrt{p} \qquad Y_{\frac{2}{2}} = -\frac{1}{2} - \frac{1}{2}\sqrt{p}$$

Für die Viertel der Gruppe ist nach Nr. 7

$$Y_{\frac{1}{4}} + Y_{\frac{2}{4}} = -\frac{1}{2} + \frac{1}{2}\sqrt{p}$$

$$Y_{\frac{1}{4}}\, Y_{\frac{2}{4}} = -2^{r-4} = -16$$

folglich

$$Y_{\frac{1}{4}} = -\frac{1}{4} + \frac{1}{4}\sqrt{p} + \frac{1}{4}\sqrt{2p - 2\sqrt{p}}$$

$$Y_{\frac{2}{4}} = -\frac{1}{4} + \frac{1}{4}\sqrt{p} - \frac{1}{4}\sqrt{2p - 2\sqrt{p}}$$

Ebenso findet sich

$$Y_{\frac{3}{4}} = -\frac{1}{4} - \frac{1}{4}\sqrt{p} + \frac{1}{4}\sqrt{2p + 2\sqrt{p}}$$

$$Y_{\frac{4}{4}} = -\frac{1}{4} - \frac{1}{4}\sqrt{p} - \frac{1}{4}\sqrt{2p + 2\sqrt{p}}$$

Für die Achtel ergiebt sich, wenn man die Formeln aus Nr. 8 nach Nr. 18 zusammenzieht,

$$Y_{\frac{1}{8}} = \frac{1}{2}\, Y_{\frac{1}{4}} + \frac{1}{2}\sqrt{Y_{\frac{1}{4}}^2 - 8\,Y - 12\,Y_{\frac{2}{2}} - 8\,Y_{\frac{2}{4}}}$$

$$Y_{\frac{2}{8}} = \frac{1}{2}\, Y_{\frac{1}{4}} - \frac{1}{2}\sqrt{Y_{\frac{1}{4}}^2 - 8\,Y - 12\,Y_{\frac{2}{2}} - 8\,Y_{\frac{2}{4}}}$$

oder bei gehöriger Substitution und Reduktion

$$Y_{\frac{1}{8}} \text{ und } Y_{\frac{2}{8}} = -\frac{1}{8} + \frac{1}{8}\sqrt{p} + \frac{1}{8}\sqrt{2p - 2\sqrt{p}}$$

$$\pm\frac{1}{8}\sqrt{\left\{7p-3+(p-5)\sqrt{p}+(2^7-4)\sqrt{2p-2\sqrt{p}}+2^5\sqrt{2p+2\sqrt{2p}}\right\}}$$

u. s. w.

II. Die zyklisch geordneten Funktionen.

§. 4. Die zyklisch geordneten Funktionen.

1) Die symmetrischen Funktionen der n Wurzeln $x_1, x_2 \ldots x_n$ einer Gleichung n-ten Grades, welche die absoluten Werthe der Koeffizienten dieser Gleichung darstellen, pflegt man lexikographisch zu ordnen, also beispielsweise für $n = 5$ die 10-gliedrige Funktion von zwei Dimensionen so zu schreiben

$$x_1 x_2 + x_1 x_3 + x_1 x_4 + x_1 x_5 + x_2 x_3 + x_2 x_4 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_4 x_5$$

Für die nachstehenden und manche anderen Betrachtungen ist die zyklische Anordnung vorzuziehen. Zyklisch geordnet nennen wir eine Gruppe von Gliedern $x_a x_b x_c + x_{a+1} x_{b+1} x_{c+1} + x_{a+2} x_{b+2} x_{c+2}$ + etc., worin die Zeiger jedes folgenden Gliedes um eine Einheit gegen die Zeiger des vorhergehenden Gliedes erhöht sind. Wenn man bei der Fortzählung nach dem letzten Zeiger n der Reihe $1, 2, 3 \ldots n$ wieder den ersten Zeiger 1 folgen lässt; so wiederholt sich in der zyklisch geordneten Gruppe nach n Gliedern unfehlbar das erste; eine solche Gruppe kann also höchstens n Glieder enthalten, und hieraus folgt, dass die lexikographisch geordnete Gruppe im Allgemeinen in mehrere zyklisch geordnete zerfällt. Beispielsweise zerfällt die vorstehende 10-gliedrige Gruppe in folgende zwei 5-gliedrige

$$(x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_5 + x_5 x_1)$$
$$+ (x_1 x_3 + x_2 x_4 + x_3 x_5 + x_4 x_1 + x_1 x_2)$$

2) Um alle zyklisch geordneten Gruppen und darin nicht mehr und nicht weniger als die der betreffenden symmetrischen Funktion angehörigen Glieder zu erhalten, verfährt man folgendermaassen. Wenn r die Zahl der Dimensionen der Funktion ist; so setzen wir irgend ein bestimmtes Element x_a vom Zeiger a in die erste Stelle des Anfangsgliedes $x_a x_b x_c x_d \ldots$ einer zyklisch geordneten Gruppe und bilden dieses Glied lexikographisch, also dergestalt, dass jeder spätere der Zeiger $a, b, c, d \ldots$ grösser ist, als jeder frühere (die Gleichheit zweier Zeiger ist ausgeschlossen). Das Anfangsglied bestimmt die zyklisch geordnete Gruppe; es kömmt daher nur darauf an, alle Anfangsglieder zu bestimmen, welche verschiedene Gruppen liefern. Zu dem Ende setzen wir die $r - 1$ Differenzen der benachbarten Zeiger $b - a = \alpha$, $c - b = \beta$, $d - c = \gamma$ etc. und erwägen, dass die Summe dieser Differenzen $\alpha + \beta + \gamma = d - a$ die Differenz zwischen dem letzten und dem ersten Zeiger des Anfangsgliedes ist, also höchstens $= n - 1$ sein kann.

Hiernach hat man alle verschiedenen Werthe von $r - 1$ ganzen Zahlen, deren Summe nicht grösser als $n - 1$ ist, in allen möglichen Reihenfolgen für die Differenzen der Zeiger des Anfangsgliedes einer zyklischen Gruppe anzunehmen. Dabei kann man immer $a = 1$ setzen, also zum ersten Elemente des Anfangsgliedes das Element x_1 nehmen.

Die auf diese Weise gebildeten Gruppen müssen alle verlangten Gruppen enthalten; es ist jedoch möglich, dass darunter eine der verlangten Gruppen mehrmals, sei es als selbstständige Gruppe, sei es als Theil einer Gruppe, erscheint, wenn man beachtet, dass $x_a\,x_b$ für die gesuchte Funktion denselben Werth hat, wie $x_b\,x_a$.

Im vorstehenden Beispiele ist $n-1=4$, $r=2$, also $r-1=1$; die eine in Betracht kommende Differenz α kann daher die Werthe 1, 2, 3, 4 annehmen, was folgende Gruppen ergiebt

$$\begin{array}{l} x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 \\ x_1x_3 + x_2x_4 + x_3x_5 + x_4x_1 + x_5x_2 \\ x_1x_4 + x_2x_5 + x_3x_1 + x_4x_2 + x_5x_3 \\ x_1x_5 + x_2x_1 + x_3x_2 + x_4x_3 + x_5x_4 \end{array}$$

Von diesen vier Gruppen ist die erste der vierten und die zweite der dritten gleich; es kömmt daher nur die erste und zweite in Betracht.

Die Funktion von $r=3$ Dimensionen aus $n=5$ Elementen ist, wenn wir nur die Zeiger schreiben,

123 124 125 134 135 145 234 235 245 345

Es kommen zwei Differenzen α und β in Betracht, deren Summe $\leqq 4$ sein muss. Diese Differenzen können also sein 11, 12, 13, 21, 22, 31. Hieraus entspringen folgende sechs Gruppen

123	234	345	451	512
124	235	341	452	513
125	231	342	453	514
134	245	351	412	523
135	241	352	413	524
145	251	312	423	534

Hiervon stimmt die erste mit der dritten und sechsten und die zweite mit der vierten und fünften überein; es kömmt also nur die erste und die zweite in Betracht und die gesuchte Funktion ist

$$\begin{array}{l} (x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2) \\ + (x_1x_2x_4 + x_2x_3x_5 + x_3x_4x_1 + x_4x_5x_2 + x_5x_1x_3) \end{array}$$

Für $n=4$ Elemente ist die Funktion von $r=2$ Dimensionen

$$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

Die Differenz α muss $\leqq 3$, kann also 1, 2 oder 3 sein. Diess giebt für die Zeiger folgende Werthe

12	23	34	41
13	24	31	42
14	21	32	43

Von diesen drei Gruppen fällt die erste mit der dritten zusammen, in der zweiten aber stimmt die erste Hälfte mit der zweiten überein, diese Gruppe bildet also zwei sich deckende zyklische Gruppen und die gegebene Funktion ist, zyklisch geordnet,

$$(x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1) + (x_1x_3 + x_2x_4)$$

3) Es liegt auf der Hand, dass wenn in zwei zyklischen Gruppen irgend zwei Glieder übereinstimmen, die ganzen Gruppen übereinstimmen und dass, wenn in einunderselben Gruppe zwei Glieder übereinstimmen, diese Gruppe ein Vielfaches einer unzerlegbaren zyklischen Gruppe ist, dass also vermittelst der Differenzen α, β, γ . . . leicht alle zyklischen Gruppen ermittelt werden können, aus welchen eine symmetrische Funktion besteht.

4) Die niedrigste Funktion von einer Dimension $x_1 + x_2 + \ldots + x_n$, sowie die höchste Funktion von n Dimensionen $x_1\, x_2 \ldots x_n$ ist stets zyklisch geordnet.

5) Wenn es erforderlich würde, symmetrische Funktionen mit bestimmter Wiederholung eines oder mehrerer Elemente, z. B. die Funktion $\Sigma\, x_1\, x_2^{\,2}\, x_3^{\,5}$ von 8 Dimensionen zyklisch zu ordnen; so kann Diess nach den vorstehenden Grundregeln ebenfalls leicht geschehen.

6) Die zyklisch geordnete Funktion erscheint als ein Inbegriff mehrerer unzerlegbaren oder primitiven zyklischen Gruppen von Gliedern. Wenn man in einer solchen Funktion alle Zeiger um eine Einheit erhöhet, variirt jede zyklische Gruppe für sich zyklisch; es tritt kein Glied aus der einen dieser Gruppen in eine andere über. Bei der lexikographisch geordneten Funktion ist Diess nicht der Fall, vielmehr springen bei der Erhöhung aller Zeiger um eine Einheit die Glieder durcheinander.

7) Wenn die Anzahl n der Elemente eine ungerade Primzahl ist, hat jede zyklische Gruppe einer jeden symmetrischen Funktion genau n Glieder. Da nun allgemein, auch wenn n keine Primzahl ist, die Anzahl der Kombinationen zur Klasse r aus n Elementen den Werth

$$s = \frac{n\,(n-1)\,(n-2)\,\ldots\,(n-r+1)}{1\,.\,2\,.\,3\,\ldots\,r}$$

hat; so muss, wenn n eine Primzahl ist, n ein Faktor von s, also $s = q\,n$ sein, worin

$$q = \frac{(n-1)\,(n-2)\,\ldots\,(n-r+1)}{2\,.\,3\,\ldots\,r}$$

ist. Für einen primen Werth der Anzahl n stellt sich also jede zyklisch geordnete einfache symmetrische Funktion von r Dimensionen in q primitiven zyklischen Gruppen von je n Gliedern dar (mit Ausnahme des Falles $r = n$, indem die höchste symmetrische Funktion nur das einzige Glied 1 2 3 . . . n hat). So hat z. B. die Funktion von 3 Dimensionen aus 7 Elementen überhaupt $s = \frac{7\,.\,6\,.\,5}{1\,.\,2\,.\,3} = 35$ Glieder und stellt sich, zyklisch geordnet, in 5 zyklischen Gruppen von je 7 Gliedern folgendermaassen dar

123	234	345	456	567	671	712
124	235	346	457	561	672	713
125	236	347	451	562	673	714
126	237	341	452	563	674	715
135	246	357	461	572	613	724

Für die gerade Primzahl 2 ist die zweidimensionale Funktion 12 zugleich die höchste und fällt daher unter die eben erwähnte Ausnahme, indem ihre Gliederzahl nicht gleich 2, sondern gleich 1 ist.

8) Zur direkten Bestimmung aller Anfangsglieder der verschiedenen zyklischen Gruppen oder zur Ausschliessung der nach Nr. 2 sich möglicherweise ergebenden äquivalenten Anfangsglieder verhelfen folgende Sätze, wobei wir für n eine ungerade Primzahl annehmen und $\frac{n-1}{2} = m$ setzen.

Aus der lexikographisch geordneten Komplexion $a\,b\,c\,d\,e\,\ldots\,z$ von r Elementen der n Zahlen 1, 2, 3 ... n sei vermöge der positiven Differenzen $b-a=\alpha$, $c-b=\beta$, $d-c=\gamma$, $e-d=\delta$ etc. die Komplexion $\alpha\,\beta\,\gamma\,\delta\,\ldots$ von $r-1$ Differenzen gebildet, welche nicht nothwendig lexikographisch geordnet zu sein braucht: wir nennen die letztere die Differenzkomplexion. Berücksichtigen wir noch die äussere Differenz zwischen dem ersten und dem letzten Gliede $a - z = -\zeta$, welche nothwendig negativ ist; so erhält man die r-stellige Differenzkomplexion $\alpha\,\beta\,\gamma\,\ldots\,(-\zeta)$ worin $\zeta = z - a = \alpha + \beta + \gamma + \ldots$ die Summe aller positiven Differenzen ist: wir nennen dieselbe die erweiterte Differenzkomplexion im Gegensatze zu der ersteren, welche eine engere ist.

Zerschneidet man die gegebene Komplexion und ihre erweiterte Differenzkomplexion an irgend einer Stelle und durchläuft dieselbe alsdann von dieser Stelle zyklisch; so ergiebt sich eine Komplexion und eine Differenzkomplexion, welche dieselben Elemente, wie die frühere hat; so ergiebt z. B. der Schnitt hinter b

aus $a\,b\,c\,d\,e\,\ldots\,z$ die neue $c\,d\,e\,\ldots\,z\,a\,b$

und $\alpha\,\beta\,\gamma\,\delta\,\ldots\,(-\zeta)$ die neue $\gamma\,\delta\,\ldots\,(-\zeta)\,\alpha\,\beta$

Die neue Komplexion besteht aus zwei lexikographisch geordneten Theilen, auf deren Grenze sich eine negative Differenz $-\zeta$ befindet; die Summe aller Differenzen ist stets gleich null.

Die alte und die neue Komplexion enthalten dieselben Elemente $a, b, c\,\ldots$, nur in zyklisch verstellter Reihenfolge, und diejenige, deren negative Differenz die äussere ist, welche also nur positive innere Differenzen hat, ist lexikographisch geordnet. Ist also eine Komplexion $c\,d\,e\,\ldots\,z\,a\,b$ bekannt, deren erweiterte Differenzkomplexion $\gamma\,\delta\,\ldots\,(-\zeta)\,\alpha\,\beta$ nur eine einzige negative Differenz $-\zeta$ enthält; so lässt sich daraus sofort das Anfangsglied einer zyklischen Gruppe bilden, indem man die auf die negative Differenz folgenden Differenzen voranstellt, also $\alpha\,\beta\,\gamma\,\delta\,\ldots\,(-\zeta)$ schreibt. Die beiden Komplexionen, deren erweiterte Differenzkomplexionen auf Verschiebung beruhen, enthalten dieselben Elemente $a, b, c\,\ldots$ in zyklischer Verschiebung. Wegen der Gleichheit der Elemente gehören sie zwar nicht einundderselben zyklischen Gruppe an, sind jedoch, da sie in den symmetrischen Funktionen nur als Produkte in Betracht kommen, äquivalent.

9) Die aus der Komplexion $a\,b\,c\,d\,e\,\ldots$ gebildete zyklische Reihe wird ein Glied enthalten, in dessen Differenzkomplexion nur Differenzen

eintreten, welche nicht grösser als m sind. Denn angenommen, die Differenzkomplexion $\alpha\ \beta\ \gamma\ \delta\ \varepsilon\ \ldots$ enthalte Differenzen $> m$; so kann sie doch nur eine einzige Differenz dieser Art, z. B. $\gamma = d - c = m + x$ enthalten, weil nach Nr. 1 die Summe aller Differenzen $\leqq 2m$ ist. Der absolute Werth ζ der äusseren Differenz ist jetzt entschieden $> m$. Erhöhet man alle Elemente der Komplexion $a\ b\ c\ d\ e\ \ldots$ um den Betrag $n + 1 - d$ (was einem Fortschritte um ebensoviel Glieder in der zyklischen Reihe entspricht); so wird dieselbe $(a + n + 1 - d)\ (b + n + 1 - d)\ (c + n + 1 - d)\ (d + n + 1 - d)\ (e + n + 1 - d)\ldots$ Von diesen Elementen werden diejenigen, welche an die Stelle von d treten, gleich 1, alle übrigen aber bleiben $\leqq n$. Die Differenzkomplexion wird also $\alpha\ \beta\ (-(n-\gamma))\ \delta\ \varepsilon\ \ldots$, d. h. an die Stelle der früheren positiven Differenz γ tritt immer die negative Differenz, deren absoluter Betrag $n - \gamma \leqq m$ ist, während alle übrigen Differenzen $\alpha, \beta, \delta, \varepsilon\ \ldots$ der engeren Differenzkomplexion ungeändert, also $< m$ bleiben, die äussere Differenz wird jetzt positiv und, da sie den absoluten Werth ζ der früheren äusseren Differenz zum Werthe n ergänzt, $\leqq m$.

Da die Differenz γ nur einmal in der gegebenen Komplexion vorkömmt; so erscheint die negative Differenz $-(n-\gamma)$ auch nur einmal in der abgeleiteten erweiterten Differenzkomplexion: verschiebt man daher darin die Differenzen so, dass die negative Differenz hinter das letzte Glied fällt, setzt man also an die Stelle von $\alpha\ \beta\ (-\xi)\ \delta\ \varepsilon\ \ldots$ die erweiterte Differenzkomplexion $\delta\ \varepsilon\ \ldots\ \alpha\ \beta\ (-\xi)$; so ist $\delta\ \varepsilon\ \ldots\ \alpha\ \beta$ eine engere Differenzkomplexion von lauter positiven Zahlen $\leqq m$, deren zugehörige Komplexion von Elementen $a, b, c\ \ldots$ dieselben Elemente wie die erstere, jedoch in zyklisch verstellter Ordnung enthält.

10) Denkt man sich alle n Elemente $1, 2, 3\ \ldots\ n$ in natürlicher Reihenfolge im Kreise aufgestellt; so kann der absolute Abstand zwischen irgend zwei Elementen nicht grösser als m sein, wenn man diesen Abstand nach derjenigen Seite der Kreislinie misst, wo er am kürzesten ist. Ist nämlich die Differenz zweier Elemente $a - b = \pm\alpha$; so ist α der fragliche Abstand, insofern $\alpha \leqq m$ ist, sodass aber, also wenn $\alpha > m$ ist, ist $n - \alpha$ der absolute Abstand, und derselbe ist dann entschieden $\leqq m$. Wir wollen jedoch im Nachstehenden nicht die absoluten, sondern, wenn es sich um mehr als zwei Elemente handelt, die Abstände in Betracht ziehen, welche zwischen den Elementen liegen, wenn man stets in derselben Richtung im Kreise von dem einen Elemente zu dem benachbarten Elemente schreitet, ohne dabei auf ein anderes Element zu stossen. Ordnet man eine gegebene Komplexion $a\ b\ c\ \ldots$ von r Elementen so, dass man, von irgend einem Elemente a_1 anfangend, erst dasjenige Element a_2, welches den Nachbar von a_1 nach der positiven zyklischen Zählrichtung darstellt, sodann das in derselben Richtung benachbarte Element a_2 u. s. w. folgen lässt, sodass also $a_1\ a_2\ a_3\ \ldots\ a_r$ dieselben Elemente wie $a\ b\ c\ \ldots$, jedoch in zyklischer Reihenfolge enthält; so wird diese Komplexion entweder aus einem einzigen oder aus zwei lexikographisch geordneten Theilen bestehen, im ersteren Falle also lauter positive und im letzteren Falle eine negative Differenz enthalten, und man kann stets dafür sorgen, dass zwischen dem ersten und letzten Elemente a_1 und a_r ein äusserer Abstand liegt, welcher entweder

grösser ist, als jeder Abstand zwischen zwei benachbarten Elementen $a_1, a_2, a_3, a_4 \ldots a_r$, oder doch ebenso gross, als der grösste der hierunter vorkommenden Abstände. Man braucht zu diesem Zwecke nur die Abstände zwischen allen benachbarten Elementen $a_1 a_2, a_2 a_3, a_3 a_1, \ldots a_r a_1$ zu betrachten und, wenn hierunter etwa die Nachbarelemente a und b den grössten Abstand haben, die Komplexion mit dem zweiten Elemente b zu beginnen.

Die Summe aller inneren Abstände und der äussere Abstand ergänzen sich zu dem ganzen Kreisumfange oder zur Anzahl n. Wenn man die Reihe aller Abstände mit Einschluss des äusseren Abstandes, welcher die letzte Stelle dieser Reihe einnimmt, verschiebt oder dieselbe mit einem beliebigen Abstande beginnt, sodass der letzte Abstand immer für den äusseren gilt; so sind die zugehörigen Komplexionen unter einander äquivalent. So liefern z. B. für $r = 4$ die vier Abstände $\alpha, \beta, \gamma, \delta$, deren Summe $\alpha + \beta + \gamma + \delta = n$ ist, in den Stellungen $\alpha\beta\gamma\delta$, $\beta\gamma\delta\alpha$, $\gamma\delta\alpha\beta$, $\delta\alpha\beta\gamma$ vier äquivalente Komplexionen. Da alle Abstände positive Grössen sind; so können die ersten $r - 1$ Abstände in jeder dieser Reihen mit Ausschluss des letzten als positive Differenzen gelten, d. h. $\alpha\beta\gamma$, $\beta\gamma\delta$, $\gamma\delta\alpha$, $\delta\alpha\beta$ bezeichnen Differenzkomplexionen, welche lexikographisch geordneten äquivalenten Komplexionen $a\,b\,c\,d$ entsprechen. Beispielsweise hat man für $n = 7$, $r = 4$ die vier Abstände 1, 2, 1, 3, deren Summe $= 7$ ist. Demnach liefern die erweiterten Abstandskomplexionen 1213 2131 1312 3121 äquivalente Komplexionen, welchen die engeren Differenzkomplexionen 121 213 131 312 entsprechen. Diese Komplexionen sind 1245 1347 1256 1457, welche sich in der That als äquivalent erweisen.

11) Ist der äussere Abstand der Komplexion $a_1\ a_2 \ldots a_r$ ein Maximum; so ist der innere Abstand von a_1 über $a_2, a_3 \ldots$ bis a_r ein Minimum, da äusserer und innerer Abstand stets $= n$ sind. Hat aber die Komplexion $a_1\ a_2 \ldots a_r$ mit der Minimalausdehnung noch eine negative Differenz, steht also das höchste Element nicht am Ende; so braucht man nur alle Elemente um den Betrag $n + 1 - a_1$ zu erhöhen, um die äquivalente Komplexion zu bekommen, welche mit dem Elemente 1 beginnt, lauter positive Differenzen $\leq m$ hat, also lexikographisch geordnet ist und zugleich die kleinste mögliche Strecke des Kreisumfanges oder der Zahlenreihe 1, 2, 3 . . . n umspannt, mithin aus den denkbar niedrigsten Elementen besteht.

12) Wenn der äussere Abstand einen Werth ζ hat, welcher unter den inneren Differenzen $\alpha, \beta, \gamma \ldots \varphi$ vorkömmt; so liefern alle diejenigen Differenzkomplexionen, bei welchen man die Differenzen $\alpha, \beta, \gamma \ldots \varphi, \zeta$ so verschiebt, dass irgend eines der darin vorkommenden ζ in den äusseren Abstand fällt, äquivalente Komplexionen. Hätte man z. B. als innere und äussere Abstände die Reihe $\alpha\beta\zeta\gamma\zeta\delta\varepsilon\zeta$; so würden die Differenzkomplexionen $\alpha\beta\zeta\gamma\zeta\delta\varepsilon$, ferner $\delta\varepsilon\zeta\alpha\beta\zeta\gamma$, sowie $\gamma\zeta\delta\varepsilon\zeta\alpha\beta$ äquivalente Komplexionen $a\,b\,c\,d\,e\,f\,g\,h$ ergeben. Denn entspricht für $a = 1$ die Differenzkomplexion $\alpha\beta\zeta\gamma\zeta\delta\varepsilon$ der Komplexion $1\,b\,c\,d\,e\,f\,g\,h$ und die Differenzkomplexion $\delta\varepsilon\zeta\alpha\beta\zeta\gamma$ der Komplexion $1\,b'\,c'\,d'\,e'\,f'\,g'\,h'$; so verwandelt sich die letztere durch Erhöhung aller Elemente um

$n + 1 - d'$ in $f g h 1 b c d e$, welche dieselben Elemente enthält wie die erste Komplexion.

13) Die aus r Elementen $a_1, a_2, a_3 \ldots a_r$ bestehende Komplexion, welche der Abstandskomplexion der r Abstände $\delta_1, \delta_2, \delta_3 \ldots \delta_{r-1}, \delta_r$ dergestalt entspricht, dass $\delta_1, \delta_2 \ldots \delta_{r-1}$ die $r - 1$ inneren Abstände und δ_r den äusseren Abstand bezeichnet, kann durch folgende Schreibweise

$$\begin{matrix} a_1 & & a_2 & & a_3 & & \ldots & & a_{r-1} & & a_r \\ & \delta_1 & & \delta_2 & & \delta_3 & \ldots & \delta_{r-1} & & \delta_r & \end{matrix}$$

dargestellt werden. Nach den vorstehenden Sätzen kann diese Komplexion stets auf eine äquivalente Form reduzirt werden, in welcher jeder innere Abstand höchstens gleich m und auch höchstens gleich dem äusseren Abstande δ_r ist. Wenn also δ irgend einen inneren Abstand bezeichnet; so gelten für die verschiedenen, nicht äquivalenten Komplexionen in reduzirter Form zunächst die Bedingungen $\delta \leqq m$ und auch $\leqq \delta_r$. Ferner gilt die Bedingung, dass sich alle inneren und äusseren Abstände zum Werthe n ergänzen, dass also die Abstandskomplexion ohne den äusseren Abstand δ_r eine beliebig variirte Kombination von $r - 1$ Elementen $\delta_1, \delta_2, \delta_3 \ldots \delta_{r-1}$ zur Summe $S = \delta_1 + \delta_2 + \ldots + \delta_{r-1}$ ist, für welche man $S = n - \delta_r = 2m + 1 - \delta_r$ hat. Da nun keiner der in S enthaltenen Abstände den Werth δ_r übersteigen kann; so ist der höchstmögliche Werth von S gleich $(r - 1)\,\delta_r$, und weil sich derselbe mit δ_r zu n ergänzen muss; so ist für den kleinstmöglichen Werth des äusseren Abstandes $(r - 1)\,\delta_r + \delta_r$ oder $r\,\delta_r = n$; und es gilt mithin für δ_r die Bedingung $\delta_r \geqq \frac{n}{r}$.

Solange $\delta_r > m$ ist, kann unter den inneren Abständen keiner vorkommen, welcher dem äusseren Abstande gleich wäre. Alle reduzirten Komplexionen, für welche der äussere Abstand $> m$ ist, sind daher durchaus verschieden. Sobald $\delta_r \leqq m$ wird, kann unter den inneren Abständen der äussere Abstand ein- oder mehreremal vorkommen. Kömmt er darin x-mal vor; so giebt es stets ausser der gegebenen noch x äquivalente reduzirte Formen, in welchen die r Abstände $\delta_1, \delta_2 \ldots \delta_r$ ein- und dieselbe zyklische Reihe bilden. Wenn aus allen reduzirten Formen diese äquivalenten gestrichen werden, bleiben alle möglichen verschiedenen Formen zurück. Die reduzirten Formen lassen sich aber nach den bezeichneten Bedingungen sämmtlich herstellen und von den äquivalenten befreien; es lassen sich also alle verschiedenen Formen, deren Anzahl nach Nr. 7 gleich q ist, durch ein direktes Verfahren herstellen. Zu dem Ende bildet man als erste Abtheilung von Abstandskomplexionen für den äusseren Abstand $\delta_r = n - r + 1$ die $(r - 1)$-stelligen Kombinationen zur Summe $r - 1$ aus den Elementen $1, 2 \ldots m$ mit beliebiger Wiederholung und Permutirung der Elemente, sodann für $\delta_r = n - r$ zur Summe r, dann für $\delta_r = n - r - 1$ zur Summe $r + 1$ u. s. w., endlich für $\delta_r = m + 1$ zur Summe m.

Alle Formen dieser Abtheilung liefern verschiedene Komplexionen. Hierauf bildet man als zweite Abtheilung die $(r - 1)$-stelligen Kombinationen für $\delta_r = m$ zur Summe $m + 1$ aus den Elementen $1, 2 \ldots m$,

alsdann für $\delta_r = m - 1$ zur Summe $m + 2$ aus den Elementen 1, 2 ... $(m - 1)$, sodann für $\delta_r = m - 2$ zur Summe $m + 3$ aus den Elementen 1, 2 ... $(m - 2)$ u. s. w., zuletzt für $\delta_r \geqq \frac{n}{r}$ zur Summe $\leqq n - \frac{n}{r}$ aus den Elementen 1, 2 ... $\left(\geqq \frac{n}{r}\right)$, indem man die letzteren Ungleichheitszeichen so versteht, dass damit der dem genauen Ausdrucke zunächst liegende ganze Werth bezeichnet sein soll. In der zweiten Abtheilung kommen äquivalente Formen vor, welche sich durch die Übereinstimmung der zyklischen Reihenfolge kennzeichnen und daher leicht ausgeschieden werden können. Wir verdeutlichen diese beiden Abtheilungen der Abstandskomplexionen durch folgende Tafel.

Elemente δ der $(r-1)$-stelligen Kombinationen	Summe S	Äusserer Abstand δ_r
1 bis m	$r - 1$	$n - r + 1$
1 „ m	r	$n - r$
1 „ m	$r + 1$	$n - r + 1$
	.	.
	.	.
	.	.
1 „ m	m	$m + 1$
1 bis m	$m + 1$	m
1 „ $m - 1$	$m + 2$	$m - 1$
1 „ $m - 2$	$m + 3$	$m - 2$
	.	.
	.	.
	.	.
1 „ $\left(\geqq \frac{n}{r}\right)$	$\leqq n - \frac{n}{r}$	$\geqq \frac{n}{r}$

Wenn auf diese Weise alle reduzirten Abstandskomplexionen ermittelt sind, ergeben sich daraus leicht die zugehörigen r-stelligen Komplexionen, indem man als erstes Element die Zahl 1 annimmt und die Abstände $\delta_1, \delta_2, \ldots \delta_{r-1}$ als Differenzen behandelt, also daraus die Komplexion

$$1 \quad (1 + \delta_1) \quad (1 + \delta_1 + \delta_2) \quad (1 + \delta_1 + \delta_2 + \delta_3) \ldots$$

herstellt.

14) Beispielsweise liefert die Primzahl $n = 11$, also $m = 5$ für alle möglichen Werthe von r folgende Tafeln.

r	Elemente ϑ	Summe S	Äusserer Abstand ϑ_r	Minimum von ϑ_r
1	1 bis 5	0	11	$\vartheta_r \geqq \frac{11}{1} = 11$
2	1 bis 5	1	10	
		2	9	
		3	8	
		4	7	
		5	6	$\vartheta_r \geqq \frac{11}{2} = 6$
3	1 bis 5	2	9	
		3	8	
		4	7	
		5	6	
	1 „ 5	6	5	
	1 „ 4	7	4	$\vartheta_r \geqq \frac{11}{3} = 4$
4	1 bis 5	3	8	
		4	7	
		5	6	
	1 „ 5	6	5	
	1 „ 4	7	4	
	1 „ 3	8	3	$\vartheta_r \geqq \frac{11}{4} = 3$
5	1 bis 5	4	7	
		5	6	
	1 „ 5	6	5	
	1 „ 4	7	4	
	1 „ 3	8	3	$\vartheta_r \geqq \frac{11}{5} = 3$

r	Elemente ϑ	Summe S	Äusserer Abstand δ_r	Minimum von δ_r
6	1 bis 5	5	6	
	1 „ 5	6	5	
	1 „ 4	7	4	
	1 „ 3	8	3	
	1 „ 2	9	2	$\delta_r \geqq \frac{11}{6} = 2$
7	1 bis 5	6	5	
	1 „ 4	7	4	
	1 „ 3	8	3	
	1 „ 2	9	2	$\delta_r \geqq \frac{11}{7} = 2$
8	1 bis 4	7	4	
	1 „ 3	8	3	
	1 „ 2	9	2	$\delta_r \geqq \frac{11}{8} = 2$
9	1 bis 3	8	3	
	1 „ 2	9	2	$\delta_r \geqq \frac{11}{9} = 2$
10	1 bis 2	9	2	$\delta_r \geqq \frac{11}{10} = 2$
11	1	10	1	$\delta_r \geqq \frac{11}{11} = 1$

Führt man die Rechnung für $r = 2$ aus (die nach Nr. 7 überhaupt 5 verschiedene zweistellige Komplexionen liefern muss); so erhält man nach vorstehender Tafel die fünf Abstandskomplexionen 1, 2, 3, 4, 5, also die fünf gesuchten Komplexionen 12, 13, 14, 15, 16.

Für = 3 (was nach Nr. 7 überhaupt 15 verschiedene Formen liefern muss), ergeben sich in der ersten Abtheilung, wenn wir die Kombinationen

zu derselben Summe durch vertikale Striche trennen, die Abstandskomplexionen

| 11 | 12, 21 | 13, 22, 31 | 14, 23, 32, 41 |

und in der zweiten Abtheilung, indem wir den äusseren Abstand durch einen Punkt von den inneren Abständen trennen,

| 15.5, 24.5, 33.5, 42.5, 51.5 | 34.4, 43.4 |

In der ersten Klammer ist die letzte Form 515 zyklisch der ersten 155 und in der zweiten Klammer ist ebenfalls die letzte 434 der ersten 344 gleich. Lässt man also von den äquivalenten Formen immer nur eine stehen; so ergeben sich die gesuchten 15 Abstandskomplexionen 11, 12, 21, 13, 22, 31, 14, 23, 32, 41, 15, 24, 33, 42, 34, welchen die nachstehenden verschiedenen Komplexionen entsprechen 123, 124, 134, 125, 135, 145, 126, 136, 146, 156, 127, 136, 147, 157, 148.

15) Nach Nr. 7 ist q die Anzahl der primitiven zyklischen Gruppen einer symmetrischen Funktion von r Dimensionen aus n Elementen. Bildet man sämmtliche symmetrischen Funktionen aus n Elementen zu den Klassen $r = 1, 2, 3 \ldots n$; so ist die gesammte Anzahl der primitiven Gruppen in den ersten $n - 1$ Klassen

$$1 + \frac{n-1}{2} + \frac{(n-1)(n-2)}{2.3} + \ldots + \frac{(n-1)(n-2)\ldots 2}{2.3\ldots(n-1)}$$

$$= \frac{1}{n}\left\{n + \frac{n(n-1)}{1.2} + \frac{n(n-1)(n-2)}{1.2.3} + \ldots + \frac{n(n-1)\ldots 2}{1.2\ldots(n-1)}\right\}$$

$$= \frac{1}{n}(2^n - 2) = \frac{2(2^{n-1} - 1)}{n}$$

Wegen der letzten Klasse von r Dimensionen, welche nur eine Reihe darstellt, ist also die Gesammtzahl aller primitiven Reihen

$$q' = \frac{2(2^{n-1} - 1)}{n} + 1$$

So bestehen z. B. für $n = 7$ die symmetrischen Funktionen von 1, 2, 3, 4, 5, 6, 7 Dimensionen aus resp. 1, 3, 5, 5, 3, 1, 1, im Ganzen aus $q' = \frac{2(2^6 - 1)}{7} + 1 = 19$ primitiven Reihen.

Dass für eine Primzahl n die Grösse q' stets eine ganze Zahl ist, leuchtet ein, da alsdann $2^{n-1} \equiv 1 \ mod\ n$ ist.

16) Wenn n eine zusammengesetzte Zahl ist, erhält man durch das in Nr. 13 beschriebene Verfahren, indem man für ein paares n unter m den Werth $\frac{n}{2}$ versteht, alle diejenigen Komplexionen, unter welchen sich die gesuchten nicht äquivalenten befinden; es können darunter alsdann aber einige äquivalente vorkommen, und zwar solche, welche keine zyklischen Gruppen von n, sondern von weniger als n Gliedern bilden.

Da sich nach n Gliedern stets das erste Glied einer zyklischen Gruppe wiederholen muss, also die Gliederzahl einer kürzeren Gruppe nur ein Faktor von n sein kann; so sind Gruppen von geringerer Gliederzahl nur möglich, wenn n eine zusammengesetzte Zahl $n'b$ und zugleich r eine Zahl $n'c$ mit einem gemeinschaftlichen Faktor n' ist, wenn also n und r ein gemeinschaftliches Maass n' haben. Denn nur, wenn $r = n'c$ ist, kann sich die erweiterte Abstandskomplexion von r Gliedern in n' gleiche Theilkomplexionen von je c Elementen zerlegen, also die Bedingung erfüllen, dass sich in der zyklischen Gruppe das erste Glied früher, als nach n Gliedern wiederholt. Da aber die Summe aller r Abstände, also das n'-fache der Summe b dieser c Elemente stets gleich n ist; so muss zugleich $n = n'b$ sein.

Hieraus geht hervor, dass wenn n und r kein gemeinschaftliches Maass haben, von kürzeren, als n-gliedrigen Perioden überhaupt keine Rede ist. Dass für diesen Fall die Gesammtzahl s aller Kombinationen aus Nr. 7 stets ein Vielfaches von n, also q eine ganze Zahl ist, ergiebt sich, wenn man

$$s = \frac{(n-1)\ (n-2)\ \ldots\ (n-r+1)}{1\ .\ 2\ \ldots\ (r-1)} \cdot \frac{n}{r}$$

schreibt und beachtet, dass der erste Faktor von s ein Binomialkoeffizient, also eine ganze Zahl v, mithin $s = \frac{v\,n}{r}$ ist, dass aber, wenn n und r relativ prim sind, r in v enthalten, also $s = q\,n$ sein muss.

Sobald jedoch n und r ein gemeinschaftliches Maass n' haben, sind unter den nach Nr. 13 gefundenen Abstandskomplexionen (nachdem von allen als äquivalent erachteten nur je eine beibehalten ist), diejenigen aufzusuchen, in welchen sich n'-mal dieselbe Theilkomplexion von $\frac{r}{n'} = c$ Zahlen wiederholt. Alle diese sind einander äquivalent, es ist also von ihnen nur eine beizubehalten; dieselbe liefert aber eine zyklische Gruppe von nur $\frac{n}{n'} = b$ Gliedern (worin b zugleich die Summe der c Zahlen der Theilgruppe darstellt).

Verschiedene Theilkomplexionen von c Zahlen mit derselben Summe b liefern immer eine selbstständige Gruppe von b Gliedern.

Für jeden besonderen gemeinschaftlichen Faktor n' der beiden Zahlen n und r ist die vorstehende Ermittlung für sich anzustellen, und es darf dabei der Fall nicht übersehen werden, wo vielleicht r selbst in n enthalten ist, also den grössten gemeinschaftlichen Faktor bildet, für welchen die Theilkomplexion eine einzige Zahl $\frac{n}{r}$ ist oder alle Abstände einander gleich sind.

Beispielsweise haben für $n = 12$, $r = 6$ die beiden Zahlen n und r das gemeinschaftliche Maass $n' = 2$, 3 und 6. Für $n' = 2$ kommen die erweiterten Abstandskomplexionen in Betracht, welche aus Theilkomplexionen von 3 Zahlen mit der Theilsumme 6 bestehen. Diese Abstandskomplexionen sind 123123, 132132 und 114114 (die Komplexionen

231231, 321321 sind resp. der ersten und der zweiten äquivalent und die Komplexionen 141141 und 411411 sind der dritten äquivalent, da in ihnen dieselbe zyklische Reihe liegt). Jede der drei genannten Abstandskomplexionen liefert ein Anfangsglied zu einer 6-gliedrigen Gruppe: diese Anfangsglieder sind 1 2 4 7 8 10, 1 2 5 7 8 11 und 1 2 3 7 8 9.

Dem gemeinschaftlichen Theiler 3 entsprechen die Theilkomplexionen von 2 Zahlen mit der Theilsumme 4, also die Abstandskomplexion 131313 (die Komplexion 313131 ist ihr äquivalent). Dieselbe liefert eine 4-gliedrige Gruppe, deren Anfangsglied 1 2 5 6 9 10 ist.

Dem gemeinschaftlichen Theiler 6 endlich entspricht die Theilkomplexion von einer Zahl mit der Theilsumme 2, also die Abstandskomplexion 2 2 2 2 2 2. Dieselbe liefert eine 2-gliedrige Gruppe, deren Anfangsglied 1 3 5 7 9 11 ist.

Im Ganzen kommen $s = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 924$ Komplexionen in Betracht. Die obengenannten Gruppen enthalten $3 \cdot 6 + 1 \cdot 4 + 1 \cdot 2 = 24$ Glieder. Alle übrigen Glieder formiren sich zu 6-gliedrigen Gruppen; es wird also noch $\frac{s - 24}{6} = 150$ Gruppen von je 6 Gliedern geben, welche sich durch das Verfahren in Nr. 13 herausstellen werden, indem man hier $m = 6$ setzt.

17) Wenn man die Zeiger einer zyklisch geordneten primitiven symmetrischen Gruppe von n' Gliedern nicht um die Differenz 1, sondern um eine beliebige Differenz α, welche relativ prim zu n' ist, wachsen lässt; so ergiebt sich eine Gruppe, welche nicht allein ebenso viel, sondern auch dieselben Glieder enthält, als die ursprüngliche: sie kann sich von dieser nur durch die Reihenfolge der Glieder und durch die Reihenfolge der Elemente in den einzelnen Gliedern oder Komplexionen unterscheiden, ist aber für die Differenz α zyklisch gebildet und, wenn die beiden Zahlen $\frac{n}{n'}$ und n' relativ prim sind, giebt es Werthe von α, für welche sich beim Überschreiten des letzten Gliedes das erste Glied identisch nach der Reihenfolge seiner Elemente herstellt.

So hat man z. B. für $n = 15$ die fünfgliedrige dreidimensionale Funktion

1 6 11 2 7 12 3 8 13 4 9 14 5 10 15

auf, welche bei dem Fortschritte mit der Differenz 1 das Glied 6 11 1 folgen würde, das mit dem ersten übereinstimmt. Bildet man aus dem ersten Gliede die Funktion mit der Differenz $\alpha = 2$, so ergiebt sich, da 2 relativ prim zu 5 ist, die Funktion

1 6 11 3 8 13 5 10 15 7 12 2 14 4 9

auf welche bei weiterem Fortschritte das Glied 6 11 1 folgen würde, welches mit dem ersten übereinstimmt. Die neue Funktion hat dieselben Glieder wie die erste, nur in anderer Reihenfolge, und ausserdem zeigen die Elemente in einigen Gliedern eine andere Reihenfolge. Für die

Differenz $\alpha = 3$, welche ebenfalls relativ prim zu 5 ist, erhält man die Funktion

1 6 11 4 9 14 7 12 2 10 15 5 13 3 8

auf welche bei weiterem Fortschritte das Glied 1 6 11 folgen würde, welches mit dem ersten nicht nur gleichwerthig, sondern identisch ist.

Um diesen wichtigen Satz zu beweisen, verändern wir die Gliederfolge der gegebenen Funktion so, dass wenn 1, 2, 3 ... n' die Nummern der Glieder bedeuten, jetzt resp. das Glied von der Nummer 1, $1 + \alpha$, $1 + 2\alpha$ ... in die 1., 2., 3. etc. Stelle gesetzt und, sobald man bei dieser Auszählung das Ende der Funktion erreicht, zyklisch in den Anfang übergegangen wird (was bei der zyklischen Natur der gegebenen Funktion einem Fortschritte in direkter Richtung um die gleiche Zeigerdifferenz entspricht). Da α relativ prim zu n' ist, wird man bei dieser Umstellung jedes Glied nur einmal treffen, jedoch nicht immer mit dem letzten Gliede der ursprünglichen Funktion, sondern mit irgend einem anderen schliessen. Nach der Entstehung der Glieder in der gegebenen Funktion aus ihrem ersten Gliede $x_a\ x_b\ x_c$ durch sukzessive Erhöhung der Zeiger um eine Einheit, ist dasjenige Glied, welches wir bei der Umstellung zum zweiten, dritten etc. genommen haben, resp. $x_{a+\alpha}\ x_{b+\alpha}\ x_{c+\alpha}$, $x_{a+2\alpha}\ x_{b+2\alpha}\ x_{c+2\alpha}$ etc., d. h. die neue Funktion bildet sich aus dem ersten Gliede der gegebenen Funktion durch den Fortschritt der Zeiger um die Differenz α. Nachdem man aber in dieser Neugestaltung das n'-te Glied, welches die Zeiger $a + (n' - 1)\alpha$, $b + (n' - 1)\alpha$, $c + (n' - 1)\alpha$ besitzt, erreicht hat, muss sich beim nächsten Fortschritte unfehlbar das erste Glied $x_a\ x_b\ x_c$ (wennauch in einer anderen Reihenfolge der Elemente, welche für den Werth des Gliedes irrelevant ist) wieder einstellen, weil man bei der Auszählung der Glieder aus der gegebenen Funktion nach $n' - 1$ Sprüngen ebenfalls wieder auf das erste Glied trifft. Hiernach ist die nach der Zeigerdifferenz α gebildete Funktion ebenfalls eine zyklisch geordnete und damit ist der erste Theil des ausgesprochenen Satzes bewiesen.

Was den zweiten Theil betrifft; so stellt sich nach dem eben bewiesenen Theile für jede zu n' relativ prime Zeigerdifferenz α nach n' Gliedern ein dem ersten gleichwerthiges Glied her, welches alle Elemente des ersten Gliedes, aber möglicherweise in anderer Reihenfolge enthält. Identisch wird dieses Glied mit dem ersten offenbar dann, wenn $\alpha n'$ ein Vielfaches von n oder $= \beta n$, mithin, da n' ein Faktor von n ist, die Zeigerdifferenz $\alpha = \beta \frac{n}{n'}$ genommen wird. Diese Bedingung, sowie die Voraussetzung, dass α relativ prim zu n' sei, kann stets erfüllt werden, wenn der Faktor $\frac{n}{n'}$ relativ prim zu n' ist; sie kann aber nicht erfüllt werden, wenn $\frac{n}{n'}$ und n' ein gemeinschaftliches Maass haben. Demzufolge liefert in dem obigen Beispiele, wo $n = 15$, $n' = 5$, $\frac{n}{n'} = 3$ ist, weil 5 und 3 kein gemeinschaftliches Maass haben, die Differenz $\alpha = 3$, aber auch $\alpha = 6$, $\alpha = 9$, $\alpha = 12$ eine zyklische symmetrische Funktion, welche

der gegebenen gleich ist und worin sich das erste Glied nach je 5 Gliedern identisch wiederholt. Wäre $n = 9$, $n' = 3$, $\frac{n}{n'} = 3$; so würde eine identische Wiederkehr des ersten Gliedes der Gruppe

147 258 369

für keine Zeigerdifferenz α möglich sein, vielmehr ergiebt sich als viertes Glied immer nur die Komplexion 471 oder 714, welche zwar gleichwerthig, aber nicht identisch mit 147 ist.

18) Wenn man eine zyklische Primitivgruppe von n' Gliedern mit der Zeigerdifferenz 1 über das letzte Glied hinaus fortsetzt; so kehrt unfehlbar nach n Gliedern das erste identisch wieder. Jede Gruppe von n ist offenbar nicht nur zyklisch, sondern reproduzirt auch ihr erstes Glied in identischer Zusammensetzung. Demzufolge ist eine zyklische Primitivgruppe von n' Gliedern, welche bei der Fortsetzung ihr erstes Glied nur gleichwerthig, aber nicht identisch wiedererzeugt, immer einem aliquoten Theile einer n-gliedrigen Gruppe, welche ihr erstes Glied identisch reproduzirt, gleichwerthig. Bezeichnet also G' eine Gruppe der ersten und G eine solche der zweiten Art; so ist $G' = \frac{n'}{n} G$ oder man hat $n\,G' = n'\,G$.

III. Die allgemeine Kreistheilung.

§. 5. Die Periodengleichungen für beliebige Primzahlen.

1) Die Zurückführung der Potenzen der Zahl a auf ihre kleinsten absoluten Reste von der Gesammtzahl $m = \frac{p-1}{2}$ in §. 1 und die Zurückführung der Gleichung (1) vom Grade $p-1$ auf die Gleichung (2) von halb so hohem Grade, resp. Zeiger $m = \frac{p-1}{2}$ stehen miteinander in organischem Zusammenhange. Lässt man die kleinsten positiven Reste zu; so erhält man $p-1$, also doppelt so viel Reste, und würde dann zweckmässig die Gleichung (1) ungeändert lassen, indem man jetzt statt mit den Grössen X_r mit den Grössen x^r operirt. Zur allmählichen Erniedrigung des Grades der gegebenen Gleichung kann man ein Verfahren einschlagen, welches dem in §. 1 beobachteten ganz analog ist. Hierbei hat man mit doppelt so viel und doppelt so hohen Resten zu thun. Diese Erschwerung wird zwar, weil keine negativen Exponenten von x, auch keine Subtraktionen, sondern nur Additionen dieser Exponenten nach der Formel $x^r \cdot x^s = x^{r+s}$ in Betracht kommen, in gewissem Grade kompensirt, es braucht also bei den Betrachtungen in §. 1 Nr. 6 ff. der

Zeichenwechsel nicht mehr beachtet zu werden; dagegen wird es bei jenen Betrachtungen erforderlich, den Fall mit ins Auge zu fassen, wo eine Summe zweier Reste $= p$ also $\equiv 0$ wird.

Bei der Ordnung der Grundtafel kann man folgende Regel beobachten. Wenn a eine primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \ mod\ p$ ist; so werden die $p - 1 = 2m$ positiven Reste der $p - 1$ Potenzen a^0, a^1, $a^2 \ldots a^{p-2}$ die $p - 1$ Zahlen 1, 2, 3 $\ldots$ $p - 1$ umfassen und die erste Periode oder Horizontalreihe der Grundtafel einnehmen. Diese Reihe, die Grundreihe, ist zyklisch gebildet und von der Beschaffenheit, dass eine Fortsetzung der Potenzen über die letzte hinaus durch sukzessive Erhöhung des Exponenten um eine Einheit die Reste vom ersten an wiedererzeugt. Bei der Zerlegung dieser Reihe kömmt es nun darauf an, zyklische Theilgruppen von der Form

$$1 \quad b^1 \quad b^2 \ldots \mid c^1 \quad b^1c^1 \quad b^2c^1 \ldots \mid c^2 \quad b^1c^2 \quad b^2c^2 \ldots \mid \text{etc.}$$

zu bilden. Das Wesentliche dieser Form besteht darin, dass 1, b^1, b^2 $\ldots$ eine zyklische, in sich selbst wiederkehrende, 1, c^1, c^2 $\ldots$ jedoch eine solche Periode ist, welche bei der Fortsetzung über das letzte Glied hinaus nicht gerade zu ihrem ersten Gliede 1, wohl aber zu einem Gliede der ersten zyklischen Theilgruppe 1, b^1, b^2 $\ldots$ und zwar immer zu einem anderen zurückkehrt.

Wenn q irgend ein Faktor der Gliederzahl der Grundreihe ist, sodass im ersten Falle $m = qr$ und im zweiten Falle $2m = qr$ ist; so kann die Grundreihe in q Theilgruppen von je r Gliedern zerlegt werden, indem man $b = a^q$ und $c = a$ nimmt, also die zu den Exponenten 0, q, $2q$, $3q$ $\ldots$ gehörigen Reste in die erste Theilgruppe, die zu den Exponenten 1, $q + 1$, $2q + 1$, $3q + 1$ $\ldots$ gehörigen in die zweite, die zu den Exponenten 2, $q + 2$, $2q + 2$, $3q + 2$ $\ldots$ gehörigen in die dritte Theilgruppe u. s. w. stellt. Indem wir in der hiernach geordneten Gruppe diese Theilgruppen unter einander stellen, nimmt dieselbe die Form der nachstehenden Grundtafel an.

$$\begin{array}{llllll}
a^0 & a^q & a^{2q} & a^{3q} & \ldots & a^{(r-1)q} \\
a^1 & a^{q+1} & a^{2q+1} & a^{3q+1} & \ldots & a^{(r-1)q+1} \\
a^2 & a^{q+2} & a^{2q+2} & a^{3q+2} & \ldots & a^{(r-1)q+2} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
a^{q-1} & a^{2q-1} & a^{3q-1} & a^{4q-1} & \ldots & a^{rq-1}
\end{array}$$

In dieser Tafel ist jede Horizontalreihe zyklisch, und die Vertikalreihen führen immer in die Horizontalreihe und zwar in ein anderes Glied zurück.

Die so geordnete Tafel lässt sich leicht in horizontale Streifen zerlegen, in welchen alle Horizontalreihen die ursprünglich darin stehenden Glieder ohne Veränderung der Reihenfolge enthalten. Ist nämlich $q = st$ und will man die Vertikalreihe von q Gliedern in t Gruppen von je s Gliedern zerlegen; so braucht man nur in die erste Theilgruppe die mit a^0, a^t, a^{2t} $\ldots$ a^{q-t} anfangenden, in die zweite die mit a^1, a^{t+1}, a^{2t+1} $\ldots$ a^{q-t+1} anfangenden, in die dritte die mit a^2, a^{t+2}, a^{2t+2} $\ldots$

a^{q-t+2} u. s. w. anfangenden Horizontalreihen zu setzen. Diess giebt für die erste Theilgruppe die Theiltafel

$$\begin{array}{llll} a^0 & a^q & a^{2q} & \ldots \quad a^{(r-1)q} \\ a^t & a^{q+t} & a^{2q+t} & \ldots \quad a^{(r-1)q+t} \\ a^{2t} & a^{q+2t} & a^{2q+2t} & \ldots \quad a^{(r-1)q+2t} \\ \ldots & \ldots & \ldots & \ldots \\ a^{q-t} & a^{2q-t} & a^{3q-t} & \ldots \quad a^{rq-t} \end{array}$$

worin man die letzte Reihe auch $a^{(s-1)t}\ a^{(2s-1)t}\ a^{(3s-1)t} \ldots a^{(rs-1)t}$ schreiben kann.

Die zweite, dritte, vierte Theiltafel ergiebt sich aus dieser durch Erhöhung ihrer Exponenten resp. um 1, 2, 3 . . . t.

Auf diese Weise kann man fortfahren, die vertikalen Reihen der zuletzt erhaltenen Theiltafeln in immer kleinere zu zerlegen, welche sämmtlich die ursprünglichen horizontalen Reihen enthalten. Die ganze Operation ist also eine Verstellung der Horizontalreihen. Nimmt man zu t immer eine in $q = st$ enthaltene Primzahl; so gelangt man endlich dahin, dass auch das letzte s, nämlich die Zahl der in der letzten Theiltafel liegenden Horizontalreihen ebenfalls eine Primzahl ist. Die Reihenfolge der einzelnen Glieder in jeder Horizontalreihe ist für die spätere Behandlung dieser in Horizontalreihen geordneten Tafel gleichgültig und darum die Verstellung dieser Glieder in derselben Horizontalreihe, welche wir sogleich besprechen werden, bedeutungslos: denn eine solche Horizontalreihe bleibt immer in dem Sinne zyklisch, dass die sukzessive Erhöhung des Exponenten irgend eines Gliedes zu einem anderen Gliede und schliesslich zu jenem Gliede zurückführt.

Soll die zuletzt erhaltene Gesammttafel oder überhaupt die Gesammttafel, wie sie sich in irgend einem Stadium der vorstehenden Zerlegung darstellt, und damit jede Horizontalreihe von r Gliedern, wenn $r = q'\,r'$ ist, in je q' Theilgruppen von r' Gliedern zerlegt werden; so verfährt man mit jeder Horizontalreihe, wie es ursprünglich mit der Grundreihe geschehen ist, indem man a^q an die Stelle von a setzt. Hierdurch gruppiren sich die Zahlen der ersten Horizontalreihe in folgenden q' Theilen, welche wir unter einander gesetzt haben, welche man aber auch hinter einander in dieselbe Horizontalreihe stellen kann.

$$\begin{array}{llllll} a^0 & a^{q'q} & a^{2q'q} & a^{3q'q} & \ldots & a^{(r'-1)q'q} \\ a^q & a^{(q'+1)q} & a^{(2q'+1)q} & a^{(3q'+1)q} & \ldots & a^{[(r'-1)q'+1]q} \\ a^{2q} & a^{(q'+2)q} & a^{(2q'+2)q} & a^{(3q'+2)q} & \ldots & a^{[(r'-1)q'+2]q} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a^{(q'-1)q} & a^{(2q'-1)q} & a^{(3q'-1)q} & a^{(4q'-1)q} & \ldots & a^{(r'q'-1)q} \end{array}$$

Die zweite, dritte, vierte . . . Horizontalreihe entspricht der vorstehenden durch Erhöhung aller Exponenten resp. um 1, 2, 3 . . . q', und die ganze Operation stellt eine Abtheilung der Tafel durch vertikale Streifen mit einer geordneten Gruppirung der Zahlen jeder Horizontalreihe

dar, wobei alle in einer Vertikalreihe stehenden Zahlen auch ferner eine Vertikalreihe bilden.

Auf diese Weise kann man fortfahren, die horizontalen Theilgruppen in immer kleinere Gruppen zu zerlegen. Die ganze Operation ist eine Verstellung der Vertikalreihen. Nimmt man zu q' immer eine in $r = q'r'$ enthaltene Primzahl; so wird das letzte r' ebenfalls eine Primzahl werden. Durch diese und die vorhergehende Operation, also durch eine entsprechende Verstellung der Horizontalreihen und dann der Vertikalreihen kann man es dahin bringen, dass sich die Grundreihe als eine Zerlegung in alle Primfaktoren von m, resp. $2m$ darstellt.

2) Die Aufstellung der Grundtafel durch die Reste der Potenzen einer primitiven Wurzel a ist zwar nicht schwer, aber bei grossen Werthen von p und a sehr mühsam. Der bequemste Weg ist der in §. 1 bezeichnete, welcher mit der Bildung der Reste der Potenzen der Zahl 2 beginnt. Angenommen, die Verdopplung der sukzessiv entstehenden Reste ergebe die zyklische Reihe der r Reste von $1, 2, 2^2, 2^3 \ldots 2^{r-1}$, indem sich für 2^r der absolute Rest 1 wieder einstelle. Wäre zufällig r gleich $2m$; so wäre 2 eine primitive Wurzel und die Grundreihe bereits gebildet: im anderen Falle ist r ein Faktor von $2m$. Ist der zweite Faktor gleich q; so hat man für die Grundtafel q solcher Reihen zu erwarten, deren Anfangsglieder sich aus den q Potenzen $1, a, a^2, a^3 \ldots a^{q-1}$ ergeben, während man jede Horizontalreihe durch Multiplikation mit 2 bildet. Entspricht der Rest von a^q, welcher nothwendig der ersten Horizontalreihe angehört, dem Reste von 2^s; so sind die Vertikalreihen leicht so zu verstellen, dass in der ersten Horizontalreihe die Reihenfolge

$$\begin{array}{rccccc} 1 & a^q & a^{2q} & a^{3q} & \ldots & a^{(r-1)q} \\ \equiv 1 & 2^s & 2^{2s} & 2^{3s} & \ldots & 2^{(r-1)s} \end{array}$$

und damit die Tafel in der obigen Form der Grundtafel erscheint.

Als Beispiel wählen wir $p = 73$, $m = 36$. Da 5 eine primitive Wurzel der Kongruenz $x^{72} \equiv 1$ ist; so ergiebt sich für die kleinsten positiven Reste die Tafel

	0	8	16	24	32	40	48	56	64
0)	1	2	4	8	16	32	64	55	37
1)	5	10	20	40	7	14	28	56	39
2)	25	50	27	54	35	70	67	61	49
3)	52	31	62	51	29	58	43	13	26
4)	41	9	18	36	72	71	69	65	57
5)	59	45	17	34	68	63	53	33	66
6)	3	6	12	24	48	23	46	19	38
7)	15	30	60	47	21	42	11	22	44

Da $5^8 \equiv 2$ ist; so hat diese Tafel schon die Form der Grundtafel, welche wir mit G bezeichnen.

Durch die Ordnung der Horizontalreihen wird diese Tafel

1	2	4	8	16	32	64	55	37
41	9	18	36	72	71	69	65	57
25	50	27	54	35	70	67	61	49
3	6	12	24	48	23	46	19	38
5	10	20	40	7	14	28	56	39
59	45	17	34	68	63	53	33	66
52	31	62	51	29	58	43	13	26
15	30	60	47	21	42	11	22	44

und durch Ordnung der Vertikalreihen erhält man die geordnete Grundtafel der Reste, welche wir mit Y bezeichnen

1	8	64	2	16	55	4	32	37
41	36	69	9	72	65	18	71	57
25	54	67	50	35	61	27	70	49
3	24	46	6	48	19	12	23	38
5	40	28	10	7	56	20	14	39
59	34	53	45	68	33	17	63	66
52	51	43	31	29	13	62	58	26
15	47	11	30	21	22	60	42	44

Dieser Tafel der Reste entspricht folgende Tafel der Exponenten der primitiven Wurzel 5, welche wir mit E bezeichnen

0	24	48	8	32	56	16	40	64	$8u$	$4v$	$2w$
4	28	52	12	36	60	20	44	68	$8u+4$		
2	26	50	10	34	58	18	42	66	$8u+2$	$4v+2$	
6	30	54	14	38	62	22	46	70	$8u+6$		
1	25	49	9	33	57	17	41	65	$8u+1$	$4v+1$	$2w+1$
5	29	53	13	37	61	21	45	69	$8u+5$		
3	27	51	11	35	59	19	43	67	$8u+3$	$4v+3$	
7	31	55	15	39	63	23	47	71	$8u+7$		

$u \equiv$ $9u'+3.0$ $9u'+3.1$ $9u'+3.2$ $9u'+3.0+1$ $9u'+3.1+1$ $9u'+3.2+1$ $9u'+3.0+2$ $9u'+3.1+2$ $9u'+3.2+2$

$3u''$ $3u''+1$ $3u''+2$

Rechts neben dieser Tafel haben wir die leicht verständlichen Zahlformen der in jeder Horizontalreihe und in den Gruppen solcher Reihen stehenden Exponenten angegeben. Wenn die Anzahl aller Horizontalreihen $= q$ ist; so haben die Exponenten einer Horizontalreihe stets die Form $qu + t$, worin t alle Werthe von 0 bis $q - 1$ annimmt. Unter der Tafel haben wir die Werthe der Grösse u für jede Vertikalreihe und für die Gruppen solcher Reihen angegeben. Wenn r die Anzahl der Vertikalreihen ist; so hat man stets $u = ru' + t'$, worin t' alle Werthe von 0 bis $r - 1$ durchläuft. Hiernach hat ein in einer bestimmten Horizontal- und Vertikalreihe stehender Exponent die Form $qu + t = q(ru' + t') + t = qr \,.\, u' + q \,.\, t' + t$.

3) Die Multiplikationen der Grössen x^b kommen auf Additionen der Reste b der Grundtafel zurück; jedes Produkt aus r Faktoren wie $x^{b_1}\ x^{b_2} \ldots x^{b_r}$ stellt sich also in der Form $x^{b_1+b_2+\ldots+b_r}$ als ein einfaches Glied dar, dessen Exponent die Summe der Exponenten der Faktoren ist. Das Ziel ist die Darstellung der symmetrischen Funktionen der Grössen x^b: da dieselben aus zyklisch geordneten Produkten dieser Grössen bestehen; so kömmt Alles darauf an, aus Resten $b_1, b_2 \ldots b_s$ die r-gliedrigen Summen

$$b_1 + b_2 + \ldots + b_r\,, \qquad b_2 + b_3 + \ldots + b_{r+1} \text{ etc.}$$

zu bilden. Hätten dieselben die Werthe $c_1, c_2 \ldots$; so wäre die betreffende symmetrische Funktion gleich $x^{c_1} + x^{c_2} \ldots$ und hierdurch würde die symmetrische Funktion von r Dimensionen auf eine Summe von eindimensionalen Elementen zurückgeführt sein. In dieser Zurückführung besteht unsere Aufgabe.

4) Die geordnete Grundtafel Y hat immer folgende Zusammensetzung. Eine prime Anzahl Elemente bilden als Reste aufsteigender Potenzen der Wurzel a eine aufsteigende und zyklische horizontale Elementarreihe, aus einer primen Anzahl solcher Elementarreihen bildet sich aufsteigend und zyklisch eine Partialreihe, aus einer primen Anzahl solcher Partialreihen wiederum aufsteigend und zyklisch eine höhere Partialreihe u. s. f., schliesslich aus einer primen Anzahl letzter Partialreihen aufsteigend und zyklisch eine ganze Horizontalreihe. In dieser Weise ist jede Horizontalreihe der Grundtafel gebildet.

Aus einer primen Anzahl ganzer Horizontalreihen bildet sich aufsteigend und zyklisch ein horizontaler Partialstreifen, aus einer primen Anzahl solcher Streifen aufsteigend und zyklisch ein höherer Partialstreifen u. s. f. und schliesslich aus einer primen Anzahl letzter horizontalen Partialstreifen die ganze Grundtafel.

Die einzelnen Vertikalreihen und Vertikalstreifen sind nicht zyklisch gebildet, nur die ganzen Horizontalreihen und Horizontalstreifen sind es, indem beim Überschreiten des letzten Gliedes eines vertikalen Zyklus ganzer Horizontalreihen die erste Horizontalreihe in veränderter Ordnung der Elemente, nämlich so wiederkehrt, dass jede neu zu durchlaufende Vertikalreihe sich um einen bestimmten Abstand horizontal verschiebt, was einem jeden einzelnen Elemente den Fortschritt in einem Schraubengange verleihet.

Jede horizontale Partialreihe kann durch Verstellung ihrer Elemente aufsteigend und zyklisch geordnet werden und eine Elementarreihe für die höheren Partialreihen bilden. Jeder horizontale Partialstreifen von der Breite der Grundtafel kann durch Verstellung der Horizontalreihen aufsteigend und zyklisch geordnet werden, also ein Elementarstreifen für höhere Partialstreifen von der Breite der Grundtafel werden. Wenn man einen Partialstreifen von geringerer Breite zur Elementargruppe annimmt, hat man bei der vertikalen Variation von einem Streifen zum anderen die damit zugleich vor sich gehende horizontale Verschiebung zu berücksichtigen.

5) Nehmen wir an, in einer Horizontalreihe H_1 der Grundtafel Y bilden die r Reste oder Elemente $a_1, a_2, \ldots a_r$ zyklisch die Elementarreihe R_1, ferner die s Elementarreihen $R_1, R_2 \ldots R_s$ zyklisch die Partialreihe S_1, ferner die t Partialreihen $S_1, S_2 \ldots S_t$ zyklisch die höhere Partialreihe T_1 u. s. f., endlich die v Partialreihen $U_1, U_2 \ldots U_v$ die ganze Horizontalreihe H_1. In derselben Weise sei jede Horizontalreihe gebildet. Die Zahlen $r, s, t \ldots v$ seien Primzahlen (wozu auch die Werthe 1 und 2 zu rechnen sind).

Wenn b_1 und c_1 zwei beliebige Elemente irgend einer Elementarreihe R_1 sind; so liefert die Summe $b_1 + c_1$, welche wir die Kombination von b_1 und c_1 nennen und kurz $b_1 c_1$ schreiben (oder ihr kleinster positiver Rest) einen Rest f_1 in irgend einer Elementarreihe R_w der Grundtafel, insofern dieser Rest nicht $\equiv p$, also $= 0$ wird. Verschiebt man die beiden Elemente b_1 und c_1 in ihrer Elementarreihe horizontal um eine Stelle (wobei wegen der zyklischen Reihenbildung der Austritt aus der Elementarreihe an der rechten Seite einen Wiedereintritt an der linken Seite bedingt); so verschiebt sich auch der ihrer Summe $b_2 c_2$ entsprechende Rest f_1 in seiner Elementarreihe R_w um eine Stelle nach f_2: denn eine solche Verschiebung entspricht der Multiplikation der Kongruenz $a^x + a^y \equiv a^z$ mit dem Faktor a^δ oder dem Übergange zu der Kongruenz $a^{x+\delta} + a^{y+\delta} \equiv a^{z+\delta}$, wobei die Exponenten $x + \delta$, $y + \delta$, $z + \delta$ nothwendig in den Elementarreihen verbleiben, welchen resp. x, y, z angehören und die je nächsten Stellen darin bezeichnen. Ein Nullrest bleibt bei dieser Variation gleich null. Eine Kombination aller r Paare $b_1 c_1, b_2 c_2 \ldots b_r c_r$ von Resten der Elementarreihe R_1, welche sich durch horizontale Verschiebung ergeben, oder die zyklische Funktion $b_1 c_1 + b_2 c_2 + \ldots + b_r c_r$ liefert also eine volle Elementarreihe R_w von Resten $f_1, f_2, \ldots f_r$.

Nach Vorstehendem liefern alle möglichen zyklischen Funktionen aus je zwei der Elemente $a_1, a_2 \ldots a_r$ volle Elementarreihen R der Grundtafel.

Wenn die beiden Elemente b_1 und k_1 nicht einunderselben, sondern zwei verschiedenen Elementarreihen R_x und R_y der Grundtafel angehören, variirt ihr Summenrest f_1 in seiner Elementarreihe R_w ganz in vorstehender Weise, d. h. die zyklische Funktion $b_1 k_1 + b_2 k_2 + \ldots + b_r k_r$ liefert immer eine volle Elementarreihe R. Kombinirt man also die Kombination zweier Elemente $b_1 c_1$ der Elementarreihe mit einem dritten Elemente d_1 derselben Elementarreihe R_1; so ist Diess gleichbedeutend mit der Kombination des Summenrestes f_1 von $b_1 c_1$ mit d_1, d. h. man

hat $b_1 c_1 d_1 = f_1 d_1 = h_1$. Der Summenrest h_1 von $f_1 d_1$ variirt aber in einer Elementarreihe; mithin giebt die dreidimensionale zyklische Funktion $b_1 c_1 d_1 + b_2 c_2 d_2 + \ldots + b_r c_r d_r$ eine volle Elementarreihe R, und es ist leicht zu erkennen, dass jede zyklische Funktion von beliebig viel Elementen $a_1, a_2 \ldots a_r$ einer Elementarreihe, da r eine Primzahl ist, diese Funktion also nach §. 4 Nr. 7 stets r Glieder hat, sich in vollen Elementarreihen der Grundtafel, worunter sich auch Nullreihen von r Gliedern befinden können, darstellt.

Der letzte Satz ist auch unmittelbar zu demonstriren, wenn man die Summe irgend einer Kombination $b_1 c_1 d_1 \ldots = h_1$ setzt und mit der Kongruenz $a^x + a^y + a^z + \ldots \equiv a^w$, welche bei dem Übergange zu der Kombination $b_2 c_2 d_2 \ldots$ in $a^{x+\delta} + a^{y+\delta} + a^{z+\delta} + \ldots \equiv a^{w+\delta}$ übergeht, identifizirt.

Wenn die Elemente b_1 und c_1 aus zwei beliebigen Elementarreihen horizontal um r Stellen, also in die nächsten Elementarreihen verschoben werden; so verschiebt sich auch die Summe f_1 horizontal um r Stellen unter Beachtung der zyklischen Reihenfolge in die nächste Elementarreihe: denn eine solche Verschiebung entspricht der Multiplikation der Kongruenz $a^x + a^y \equiv a^z$ mit a^β oder dem Übergange zur Kongruenz $a^{x+\beta} + a^{y+\beta} \equiv a^{z+\beta}$ wobei die Exponenten $x + \beta$, $y + \beta$, $z + \beta$ in die benachbarten Elementarreihen übertreten. Eine s-malige Wiederholung dieser Verschiebung führt den Rest der Summen $b_1 c_1$, $b_{1+r} c_{1+r}$, $b_{1+2r} c_{1+2r}$ etc., nämlich die Zahlen f_1, f_{1+r}, f_{1+2r} etc. sukzessiv in alle Elementarreihen R_w, R_{w+1}, R_{w+2} ... einer Partialreihe S. Ein Nullrest bleibt bei dieser Verschiebung gleich null.

Die zyklischen Verschiebungen der Kombination $b_1 c_1$ und jeder Kombination von beliebig viel Elementen einer Elementarreihe um je eine Stelle durch alle Elementarreihen $R_1, R_2 \ldots R_s$ führt hiernach den Summenrest f_1 durch alle Elemente einer Partialreihe S der Grundtafel.

Dieser Satz gilt offenbar für jede beliebige Kombination $b_1 c_1 d_1 \ldots$ von Elementen $b_1, c_1, d_1 \ldots$ beliebiger Elementarreihen.

Vergegenwärtigt man sich jetzt die Kombinationen zweier oder mehrerer Elementarreihen $R_1, R_2 \ldots$ derselben Partialreihe S_1, z. B. die Kombination $R_1 R_2$, worunter die Kombination jedes Elementes von R_1 mit jedem Elemente von R_2 zu verstehen ist, und bildet man durch horizontale Verschiebung der Kombination $R_1 R_2$ immer um den Abstand einer Elementarreihe die zyklische Funktion $R_1 R_2 + R_2 R_3 + \ldots + R_s R_1$; so setzt sich dieselbe offenbar aus lauter zyklischen Funktionen von je zwei Elementen b_1, c_1 zusammen, welche je zwei kombinirten Elementarreihen R_1, R_2 angehören und mit sukzessiven Verschiebungen immer um eine Stelle den ganzen Weg einer Partialreihe S durchlaufen.

Jede symmetrische Funktion von beliebig vielen Elementarreihen $R_1, R_2 \ldots R_s$ einunderselben Partialreihe S_1 erscheint daher als ein Inbegriff voller Partialreihen S, worunter sich auch Nullreihen von $r s$ Gliedern befinden können.

Auf demselben Wege erkennt man, dass jede symmetrische Funktion von Partialreihen $S_1, S_2 \ldots S_t$, welche derselben höheren Partialreihe T angehören, als Inbegriff von Reihen der letzteren Ordnung, einschliess-

lich etwaiger Nullreihen erscheint, und dass schliesslich eine symmetrische Funktion von Partialreiheu U_1, U_2 ... U_v der letzten Ordnung ein Inbegriff ganzer Horizontalreihen H der Grundtafel ist, vorausgesetzt, dass r, s, t ... v lauter Primzahlen sind (weil nur unter dieser Voraussetzung nach §. 4 die Gliederzahl aller symmetrischen Funktionen oder der einzelnen primitiven zyklischen Gruppen derselben die volle ist).

6) Wie sich in horizontaler Linie aus den Elementen die Elementarreihen, aus diesen die Partialreihen und aus diesen die ganzen Horizontalreihen bilden, so bilden sich in vertikaler Linie aus den ganzen Horizontalreihen, als den Elementen, die Elementarstreifen, aus diesen die Partialstreifen und aus diesen die ganze Grundtafel, und weil diese Reihen und Streifen in ihrer Ganzheit (nicht in ihren einzelnen vertikalen Linien) zyklisch gebildet sind, die ganze Horizontalreihe bei der Bildung des Elementarstreifens also dieselbe Rolle spielt, wie vorhin eine Partialreihe bei der Bildung der nächst höheren Partialreihe; so gelten von jenen ganzen Reihen und Streifen auch die vorstehend entwickelten Sätze, wenn man sich unter a_1, a_2 ... a_r jetzt die Horizontalreihen, unter R_1, R_2 ... R_s die Elementarstreifen, unter S_1, S_2 ... S_t die ersten Partialstreifen, unter T_1, T_2 ... die nächst höheren Partialstreifen, unter U_1, U_2 ... die letzten Partialstreifen und schliesslich unter H_1 die ganze Grundtafel Y vorstellt.

Wir heben hierbei folgende Sätze hervor. Verschiebt man die Kombination zweier beliebigen Reste a_m und b_n horizontal von Stelle zu Stelle, bildet also die Summen $a_m + b_n = c_1$, $a_{m+1} + b_{n+1} = c_2$, $a_{m+2} + b_{n+2} = c_3$ u. s. w.; so durchläuft die Summe c (resp. deren Rest) endlich eine volle Horizontalreihe der Tafel, indem er unausgesetzt andere Werthe annimmt (bei dem Vorschieben der Reste a und b ist die zyklische Folge zu beachten, welche die Summe c hin und wieder zu Sprüngen in der betreffenden Horizontalreihe nöthigt). Verschiebt man die Kombination $a_m + b_n = c_1$ vertikal von Stelle zu Stelle unter Beachtung der zyklischen Folge; so treffen die Summen c_1, c_2, c_3 ... in lauter verschiedene Horizontalreihen, durchlaufen also (wennauch in Sprüngen) die ganze Höhe der Tafel. (Die bei den horizontalen und vertikalen Verschiebungen zu beobachtende Folge ist am leichtesten aus der Exponententafel E zu ersehen; sie ist dergestalt zu wählen, dass die Exponenten der beiden kombinirten Reste immer dieselbe Differenz bewahren.) Eine Verschiebung der Kombination $a_m + b_n$ in horizontaler und in vertikaler Richtung führt die Summe durch alle Reste der Grundtafel. So liefert die Verschiebung der Kombination der beiden Reste 1 und 40, welche wir kurz $1 . 40 = 41$ schreiben und welche den Exponenten 0 und 25 entsprechen, in dem obigen Beispiele folgende Reihen, in welchen die Differenz der Exponenten gleich 25, resp. $\equiv 25$ *mod* 72 ist.

1.40=41	8.28=36	64. 5=69	2. 7= 9	16.56=72	55.10=65	4.14=18	32.39=71	37.20=57	(Reihe 2)
41.34= 2	36.53=16	69.59=55	9.68= 4	72.33=32	65.45=37	18.63= 8	71.66=64	57.17= 1	(Reihe 1)
25.51= 3	54.43=24	67.52=46	50.29= 6	35.13=48	61.31=19	27.58=12	70.26=23	49.62=38	(Reihe 4)
3.47=50	24.11=35	46.15=61	6.21=27	48.22=70	19.30=49	12.42=54	23.44=67	38.60=25	(Reihe 3)
5.54=59	40.67=34	28.25=53	10.35=45	7.61=68	56.50=33	20.70=17	14.49=63	39.27=66	(Reihe 6)
59.24=10	34.46= 7	53. 3=56	45.48=20	68.19=14	33. 6=39	17.23=40	63.38=28	66.12= 5	(Reihe 5)
52.36=15	51.69=47	43.41=11	31.72=30	29.65=21	13. 9=22	62.71=60	58.57=42	26.18=44	(Reihe 8)
55.16=31	47.55=29	11. 2=13	30.32=62	21.37=58	22. 4=26	60.64=51	42. 1=43	44. 8=52	(Reihe 7)

7) Wenn daher P_α, P_β, P_γ ..., sowie P_0, P_λ, P_μ, P_ν ... Partialgruppen (Reihen oder Streifen) von derselben Ordnung bezeichnen; so wird die Kombination der ersteren Gruppen P sich als ein Inbegriff von Gruppen P in linearer Form nach der Formel

$$(1) \qquad P_\alpha P_\beta P_\gamma \ldots = \pi_0 P_0 + \pi_\lambda P_\lambda + \pi_\mu P_\mu + \pi_\nu P_\nu + \ldots$$

darstellen, worin P_0 eine Nullgruppe P, dagegen π_0, π_λ, π_μ, π_ν ... lauter ganze Zahlen sind. Angenommen, die Gruppen P_α, P_β, P_γ ... gehören einunderselben nächst höheren Gruppe Q an und die Anzahl der in einem Q enthaltenen Gruppen P sei gleich q. Verschiebt man dann in der letzteren Gruppe die Kombination $P_\alpha P_\beta P_\gamma$ ... zyklisch um eine Stelle, sodass die Zeiger α, β, γ in $\alpha + 1, \beta + 1, \gamma + 1$ übergehen (und eventuell zyklisch wiederkehren); so erhält man

$$P_{\alpha+1} P_{\beta+1} P_{\gamma+1} \ldots = \pi_0 P_0 + \pi_\lambda P_{\lambda+1} + \pi_\mu P_{\mu+1} + \pi_\nu P_{\nu+1} + \ldots$$

und allgemein für ein beliebiges u

$$(2) \qquad P_{\alpha+u} P_{\beta+u} P_{\gamma+u} \ldots = \pi_0 P_0 + \pi_\lambda P_{\lambda+u} + \pi_\mu P_{\mu+u} + \pi_\nu P_{\nu+u} + \ldots$$

Durch die fortgesetzte Verschiebung der Kombination $P_\alpha P_\beta P_\gamma$ ... in derselben Gruppe Q füllen sich endlich auf der rechten Seite die Gruppen Q, welchen die Partialgruppen P_λ, $P_{\lambda+1}$ etc., P_μ, $P_{\mu+1}$ etc., P_ν, $P_{\nu+1}$ etc. angehören. Wenn man also die zyklische Funktion $P_\alpha P_\beta P_\gamma \ldots + P_{\alpha+1} P_{\beta+1} P_{\gamma+1} \ldots + P_{\alpha+2} P_{\beta+2} P_{\gamma+2} \ldots + \ldots$ mit $F(P_\alpha P_\beta P_\gamma \ldots)$ bezeichnet; so stellt sich dieselbe durch die Addition aller Gleichungen, welche sich aus der Gl. (2) ergeben, wenn man darin nachundnach $u = 1, 2, 3 \ldots q$ setzt, und beachtet, dass $q \pi_0 P_0 = \pi_0 (q P_0) = \pi_0 Q_0$ ist, als ein Inbegriff voller Gruppen Q nach der Formel

$$(3) \qquad F(P_\alpha P_\beta P_\gamma \ldots) = \pi_0 Q_0 + \pi_\lambda Q_\lambda + \pi_\mu Q_\mu + \pi_\nu Q_\nu + \ldots$$

dar. Die Koeffizienten π_0, π_λ, π_μ, π_ν ... in dieser Gleichung sind dieselben wie in Gl. (1) und wir haben darin mit Q_λ, Q_μ, Q_ν ... diejenigen Gruppen Q bezeichnet, in welchen die Partialgruppen P_λ, P_μ, P_ν ... liegen. Gehörten also in Gl. (1) mehrere P, z. B. P_λ und P_μ derselben Gruppe Q_λ an; so würde in Gl. (3) $Q_\mu = Q_\lambda$ sein und man könnte die beiden Glieder $\pi_\lambda Q_\lambda + \pi_\mu Q_\mu$ in ein Glied $(\pi_\lambda + \pi_\mu) Q_\lambda$ zusammenziehen.

Wenn die rechte Seite für bestimmte Partialgruppen P_α, P_β, P_γ ... bekannt ist, ergiebt sich für andere Partialgruppen $P_{\alpha+u}$, $P_{\beta+u}$, $P_{\gamma+u}$ ..., welche für ein beliebiges u einer anderen Gruppe Q angehören, die Formel

$$(4) \qquad F(P_{\alpha+u} P_{\beta+u} P_{\gamma+u} \ldots) = \pi_0 Q_0 + \pi_\lambda Q_{\lambda+u} + \pi_\mu Q_{\mu+u} + \pi_\nu Q_{\nu+u} + \ldots$$

Wenn man in Gl. (4) u sukzessiv gleich u, $2u$, $3u$ ... ϱu setzt, indem ϱ die Anzahl der Gruppen Q, welche in der nächst höheren Gruppe

R enthalten sind, bezeichnet; so ergiebt eine Addition aller erhaltenen ϱ Gleichungen

$$(5) \qquad FF(P_\alpha P_\beta P_\gamma \ldots) = \pi_0 R_0 + \pi_\lambda R_\lambda + \pi_\mu R_\mu + \pi_\nu R_\nu + \ldots$$

worin R_λ, R_μ, R_ν . . . diejenigen höheren Gruppen darstellen, in welchen Q_λ, Q_μ, Q_ν . . . liegen.

Da die linke Seite einer jeden der Gleichungen (1) bis (5) ebenso viel Reste der Grundtafel enthalten muss, als die rechte Seite; so erhält man, wenn man die Anzahl der in einer Gruppe P enthaltenen Reste gleich k setzt, für das Produkt $P_\alpha P_\beta P_\gamma$ . . . von δ Dimensionen

$$k^\delta = (\pi_0 + \pi_\lambda + \pi_\mu + \pi_\nu + \ldots) k$$

mithin für die Summe σ der Koeffizienten der Gl. (1)

$$(6) \qquad \sigma = k^{\delta-1}$$

Die Koeffizienten der Gl. (1) sind auch die der Gl. (3) für eine primitive zyklische Funktion: besteht also die ganze symmetrische Funktion aus n primitiven Reihen; so nehmen die Glieder und Koeffizienten der Gl. (3) andere Werthe an und man hat

$$(7) \qquad \sigma = n k^{\delta-1}$$

Diese Formel, welche bei den späteren Ermittlungen der einzelnen Koeffizienten π_0, π_λ, π_μ . . . eine nützliche Kontrole darbietet, gilt für alle Werthe der Dimensität δ von $\delta = 1$ bis $\delta = q - 1$.

Die symmetrische Funktion von q Dimensionen hat jedoch nicht q, sondern nur ein einziges Glied $P_1 P_2 \ldots P_q$; für $\delta = q$ ergiebt sich also

$$(8) \qquad \sigma = \frac{k^\delta}{q}$$

Der letztere Fall ereignet sich, wenn $q = 2$ ist, schon bei der zweidimensionalen Funktion $P_1 P_2$.

Da die Gl. (3) für jede primitive zyklische Gruppe gilt; so hat auch jeder Inbegriff von solchen Gruppen und demzufolge jede symmetrische Funktion (§. 4) der Grössen P die auf der rechten Seite von Gl. (3) stehende Form. Ja, Diess gilt selbst für den Fall, dass q keine Primzahl ist, also die symmetrische Funktion F aus mehreren primitiven Reihen von verschiedener Gliederzahl besteht: denn, da diese Funktion bei der Erhöhung der Zeiger aller P um 1 innerhalb derselben Gruppe Q unverändert bleiben muss; so kann die rechte Seite keine Gruppen P enthalten, welche sich nicht zu lauter Gruppen von der Höhe der Q ergänzten. Übrigens werden, wenn q keine Primzahl ist, die einzelnen Koeffizienten der Gl. (3) nicht denen der Gl. (1) gleich sein, wohl aber wird ihre Summe der Summe der letzteren gleich bleiben.

Die Beobachtung der zyklischen Reihenfolge bei der Verschiebung einer Kombination, sei es in horizontaler, sei es in vertikaler Richtung, bei dem Übergange von Gl. (1) zu (2) oder von Gl. (3) zu (4) ist von grosser Wichtigkeit. Der Einblick in die Exponententafel E er-

leichtert diese Operation, und wir heben nochmals hervor, dass bei einer solchen Verschiebung die Differenz der Exponenten der in der Kombination erscheinenden Reste stets konstant bleiben muss. Ausserdem ist es nothwendig, bei einer vertikalen Verschiebung für die Zeiger $\lambda, \mu, \nu \ldots$ der Gruppen P oder Q nicht die von oben nach unten laufenden Ordnungszahlen 1, 2, 3 . . ., sondern die ersten Exponenten der Horizontalreihen (also im obigen Beispiele die Zahlen 0, 4, 2, 6, 1, 5, 3, 7) anzunehmen oder die Horizontalreihen in der Reihenfolge zu schreiben, wie sie die ursprüngliche Grundtafel G enthält, worin die Reste 1, 5, 25, 52, 41, 59, 3, 15 voranstehen, sodass also eine vertikale Verschiebung um eine Stelle oder die Variation der Zeiger um eine Einheit gleichbedeutend ist mit dem Übertritte in diejenigen Horizontalreihen, deren Exponenten um eine Einheit grösser sind, also von der 1. zu der 5., dann zu der 3., dann zu der 7., dann zu der 2., dann zu der 6., dann zu der 4. und endlich zu der 8. Reihe der Tafel Y.

8) Die im Vorstehenden erörterte Zusammensetzung der Grundtafel Y aus den Elementar- und Partialgruppen ergiebt die Auflösung der Tafel in ihre Elemente auf dem umgekehrten Wege, indem man vermittelst der letzteren Formeln von der Gesammttafel zunächst vertikal zu den aufeinanderfolgenden Partialstreifen bis zu den Horizontalreihen und sodann von diesen horizontal zu den Partialreihen und endlich zu den einzelnen Elementen oder Resten zurückschreitet. Immer ist nach der Natur des Problems die linke Seite der letzten Gleichung in Gestalt einer zyklisch geordneten symmetrischen Funktion aus einer oder mehreren Reihen von gleicher und primer Gliederzahl gegeben und die auf der rechten Seite stehenden Gruppen $Q_0, Q_\lambda, Q_\mu \ldots$ nebst deren Koeffizienten $\varkappa_0, \varkappa_\lambda, \varkappa_\mu \ldots$ sind die gesuchten Grössen. Die Bestimmung der Letzteren ist ein wesentlicher Theil der vorliegenden Abhandlung, welcher in Folgendem seine Lösung findet.

Die Kombination $P_\alpha P_\beta$ der beiden Gruppen P_α und P_β ist der Inbegriff der Reste der Summen eines jeden Elementes von P_α mit einem jeden Elemente von P_β. Bezeichnet man also die in P_α enthaltenen Reste mit $a_1, a_2, a_3 \ldots a_r$ und die in P_β enthaltenen mit $b_1, b_2, b_3 \ldots b_r$; so ist $P_\alpha P_\beta =$

$$\begin{aligned}
&a_1 b_1 + a_2 b_2 + a_3 b_3 + \ldots + a_r b_r \\
+\ &a_1 b_2 + a_2 b_3 + a_3 b_4 + \ldots + a_r b_1 \\
+\ &a_1 b_3 + a_2 b_4 + a_3 b_5 + \ldots + a_r b_2 \\
&\quad\cdot \quad\quad\cdot \quad\quad\cdot \quad\quad\cdot \quad\quad\cdot \quad\quad\cdot \\
+\ &a_1 b_r + a_2 b_1 + a_3 b_2 + \ldots + a_r b_{r-1}
\end{aligned}$$

In jeder horizontalen Reihe dieses Ausdruckes ergeben sich alle späteren Glieder durch horizontale Verschiebungen des ersten Gliedes um je eine Stelle. Da es uns nun nicht auf die Kenntniss der einzelnen Glieder, sondern auf die Kenntniss der höheren Gruppen Q ankömmt, in welchen jene Glieder volle Reihen bilden; so genügt die Kenntniss des

ersten Gliedes einer jeden dieser Reihen. Demzufolge sind die Glieder $a_1 b_1$, $a_1 b_2$, $a_1 b_3 \ldots a_1 b_r$ zu bilden, oder es ist nachzusehen, welche Summen der erste Rest a_1 der Gruppe P_α mit den einzelnen Resten $b_1, b_2 \ldots b_r$ der Gruppe P_β bildet und welche Stellen diese Summen in der Grundtafel einnehmen. Da sich jeder solche Summenrest, solange es sich um eine Kombination von Partialstreifen handelt, zu einer vollen Horizontalreihe der Grundtafel und, sobald es sich um eine Kombination von Partialreihen handelt, zu einer Partialreihe erweitert; so liefern die erwähnten Summenreste die Werthe der Inbegriffe P oder der Grössen $\pi_0 P_0$, $\pi_\lambda P_\lambda$, $\pi_\mu P_\mu$ etc., welche sich für die zyklische symmetrische Funktion $F(P_\alpha P_\beta)$ zu den Inbegriffen $\pi_0 Q_0$, $\pi_\lambda Q_\lambda$, $\pi_\mu Q_\mu$ etc. zusammensetzen.

Die Kombination $P_1 P_\varepsilon$ ergiebt nach der betreffenden Formel in Nr. 7 jede andere Kombination $P_{1+\eta} P_{\varepsilon+\eta}$, deren Zeiger $1 + \eta$ und $\varepsilon + \eta$ sich um dieselbe Differenz η von den Zeigern 1 und ε der ersten Kombination unterscheiden. Demzufolge beschränken wir die vorstehende Ermittlung auf Kombinationen der ersten Gruppe P_1 der Grundtafel mit einer anderen Gruppe P_ε. Der erste Rest a_1 der ersten Gruppe P_1 ist $= 1$; es kömmt also nur darauf an, alle Reste von P_ε um 1 zu erhöhen oder die Summen $b_1 + 1$, $b_2 + 1$, $b_3 + 1$ etc. zu bilden und deren Stellen in der Tafel zu konstatiren.

Wenn die zweidimensionale Gruppe $P_\beta P_\gamma$ bekannt geworden ist, führt eine Kombination aller Reste derselben mit dem ersten Reste 1 der Gruppe P_α zur Kenntniss der dreimensionalen Gruppe $P_\alpha P_\beta P_\gamma$ und sodann zur Kenntniss der Funktion $F(P_\alpha P_\beta P_\gamma)$.

Allgemein, führt die Gruppe $P_\beta P_\gamma P_\delta \ldots$ von x Dimensionen durch Kombination mit 1 zur Gruppe $P_\alpha P_\beta P_\gamma P_\delta \ldots$ von $x + 1$ Dimensionen und zur zyklischen symmetrischen Funktion $F(P_\alpha P_\beta P_\gamma P_\delta \ldots)$.

Um eine symmetrische Funktion von irgend einer Dimensität zu bilden, sind die Funktionen der nächst niedrigeren Dimensität bereits hergestellt: aus einem Gliede der Letzteren ergiebt sich daher das Anfangsglied der Ersteren einfach durch Erhöhung der in jener enthaltenen Reste um eine Einheit und alsdann jedes folgende Glied und die ganze Funktion durch zyklische Verschiebung. Hierdurch ist die Aufgabe der Bestimmung jeder symmetrischen Funktionen gelös't, und wir haben dieselbe nur an einem Beispiele zu erläutern.

9) Beispiel. Für die Primzahl $p = 73$ ergiebt sich folgende Zerlegung der Grundtafel. Durch den ersten Primfaktor 2 von 72 zerfällt die Tafel Y in die obere Hälfte $Y_{\frac{1}{2}}$ und die untere Hälfte $Y_{\frac{2}{2}}$. Die eindimensionale zyklisch geordnete symmetrische Funktion dieser beiden Grössen ist

$$Y_{\frac{1}{2}} + Y_{\frac{2}{2}} = Y$$

Die zweidimensionale Funktion besteht aus dem einen Gliede $Y_{\frac{1}{2}} Y_{\frac{2}{2}}$. Jede Hälfte der Grundtafel enthält 36 Reste, das Produkt aus Beiden

liefert mithin $36^2 = 1296$ Reste. Hiervon brauchen wir jedoch nur 36, nämlich die Kombinationen des ersten Restes 1 von $Y_{\frac{1}{2}}$ mit jedem Reste von $Y_{\frac{2}{2}}$ darzustellen, indem die Verschiebung einer jeden solchen Kombination durch die ganze Breite und Höhe von $Y_{\frac{1}{2}}$, also durch die ganze Breite der Tafel und durch die halbe Höhe derselben 36 Reste liefert, deren Gesammtheit volle Halbtafeln $Y_{\frac{1}{2}}$ und $Y_{\frac{2}{2}}$ ausfüllen. Die Kombinationen des Restes 1 mit 5, 40, 28, 10 . . . sind

6	41	29	11	8	57	21	15	40
60	35	54	46	69	34	18	64	67
53	52	44	32	30	14	63	59	27
16	48	12	31	22	23	61	43	45

Numeriren wir die Horizontalreihen der Tafel Y von oben herab mit 1, 2, 3, 4, 5, 6, 7, 8; so gehören die vorstehenden Reste folgenden Horizontalreihen an

4	2	7	8	1	2	8	8	5
8	3	3	4	2	6	2	1	3
6	7	8	1	8	5	6	6	3
1	4	4	7	8	4	3	7	6

Hierunter befinden sich 18 obere und 18 untere Horizontalreihen. Da sich durch die horizontale Verschiebung jeder Kombination jede dieser Horizontalreihen füllt, und da sich durch die vertikale zyklische Verschiebung jeder solchen Reihe über die Höhe der halben Tafel die betreffende Halbtafel füllt; so erscheint durch diese Verschiebung 18-mal die obere Halbtafel $Y_{\frac{1}{2}}$ und 18-mal die untere Halbtafel $Y_{\frac{2}{2}}$, im Ganzen also 18-mal die ganze Tafel Y, man hat daher für die Gl. (3) in Nr. 7

$$Y_{\frac{1}{2}}\ Y_{\frac{2}{2}} = 18\ Y$$

Jetzt handelt es sich, da der nächste Primfaktor von 72 wiederum 2 ist, um die Zerlegung der Halbtafel $Y_{\frac{1}{2}}$ in das obere und untere Viertel $Y_{\frac{1}{4}}$ und $Y_{\frac{2}{4}}$, sowie der Halbtafel $Y_{\frac{2}{2}}$ in $Y_{\frac{3}{4}}$ und $Y_{\frac{4}{4}}$. Wir bewirken zunächst die erste Zerlegung, stellen also die Kombinationen des ersten Restes 1 von $Y_{\frac{1}{4}}$ mit allen Resten 25, 54, 67, 50 etc. von $Y_{\frac{2}{4}}$ dar. Dieselben sind

26	55	68	51	36	62	28	71	50
4	25	47	7	49	20	13	24	39

und gehören folgenden Horizontalreihen an

7	1	6	7	2	7	5	2	3
1	3	8	5	3	5	7	4	5

Hierunter befinden sich 8 obere und 10 untere Horizontalreihen, und zwar sind unter den ersteren 8 Reihen 4 Reihen aus $Y_{\frac{1}{4}}$ und 4 Reihen aus $Y_{\frac{2}{4}}$ und unter den letzteren 10 Reihen sind 5 Reihen aus $Y_{\frac{3}{4}}$ und 5 Reihen aus $Y_{\frac{4}{4}}$. Durch die Horizontalverschiebung ergänzen sich alle diese Reihen zu vollen Horizontalreihen und durch die Vertikalverschiebung um die Höhe einer Vierteltafel füllen sich die Halbtafeln und man erhält nach Nr. 7 Gl. (3)

$$Y_{\frac{1}{4}}\, Y_{\frac{2}{4}} = 4\, Y_{\frac{1}{2}} + 5\, Y_{\frac{2}{2}}$$

Neben dieser zweidimensionalen Funktion besteht die eindimensionale

$$Y_{\frac{1}{4}} + Y_{\frac{2}{4}} = Y_{\frac{1}{2}}$$

Für die unteren Viertel hat man ohne Weiteres nach Gl. (4)

$$Y_{\frac{3}{4}}\, Y_{\frac{4}{4}} = 4\, Y_{\frac{2}{2}} + 5\, Y_{\frac{1}{2}}$$
$$Y_{\frac{3}{4}} + Y_{\frac{4}{4}} = Y_{\frac{2}{2}}$$

Hiernächst sind, da der dritte Primfaktor von 72 wiederum 2 ist, die Viertel wie $Y_{\frac{1}{4}}$ in die Horizontalreihen $Y_{\frac{1}{8}}$ und $Y_{\frac{2}{8}}$ zu zerlegen. Zu dem Ende bilden wir die Kombinationen des ersten Restes 1 von $Y_{\frac{1}{8}}$ mit allen Resten von $Y_{\frac{2}{8}}$

42	37	70	10	0	66	19	72	58

Dieselben liegen in den Horizontalreihen

8	1	3	5	0	6	4	2	7

Hierunter befinden sich ausser der einen Nullreihe alle Horizontalreihen, also die beiden Reihen aus $Y_{\frac{1}{4}}$, $Y_{\frac{2}{4}}$, $Y_{\frac{3}{4}}$ uud $Y_{\frac{4}{4}}$. Die Horizontalreihen ergänzen sich durch die Horizontalverschiebung, eine Vertikalverschiebung findet nicht weiter statt, man hat also, wenn man die Nullreihe mit $Y_{\frac{1}{8}}(0)$ bezeichnet, nach Gl. (3)

$$Y_{\frac{1}{8}}\, Y_{\frac{2}{8}} = Y_{\frac{1}{8}}(0) + Y_{\frac{1}{4}} + Y_{\frac{2}{4}} + Y_{\frac{3}{4}} + Y_{\frac{4}{4}} = Y_{\frac{1}{8}}(0) + Y$$

und daneben

$$Y_{\frac{1}{8}} + Y_{\frac{2}{8}} = Y_{\frac{1}{4}}$$

Für die folgenden Achtel ergiebt sich nach Gl. (4)

$$Y_{\frac{3}{8}}\, Y_{\frac{4}{8}} = Y_{\frac{1}{8}}(0) + Y \qquad Y_{\frac{3}{8}} + Y_{\frac{4}{8}} = Y_{\frac{2}{4}}$$

$$Y_{\frac{5}{8}}\, Y_{\frac{6}{8}} = Y_{\frac{1}{8}}(0) + Y \qquad Y_{\frac{5}{8}} + Y_{\frac{6}{8}} = Y_{\frac{3}{4}}$$

$$Y_{\frac{7}{8}}\, Y_{\frac{8}{8}} = Y_{\frac{1}{8}}(0) + Y \qquad Y_{\frac{7}{8}} + Y_{\frac{8}{8}} = Y_{\frac{4}{4}}$$

Für die Zerlegung der ersten Horizontalreihe $Y_{\frac{1}{8}}$ vermöge des Primfaktors 3 in die drei Partialreihen $Y_{\frac{1}{8}\cdot\frac{1}{3}}$, $Y_{\frac{1}{8}\cdot\frac{2}{3}}$, $Y_{\frac{1}{8}\cdot\frac{3}{3}}$ hat man zuvörderst die eindimensionale Funktion

$$Y_{\frac{1}{8}\cdot\frac{1}{3}} + Y_{\frac{1}{8}\cdot\frac{2}{3}} + Y_{\frac{1}{8}\cdot\frac{3}{3}} = Y_{\frac{1}{8}}$$

Das erste Glied der zweidimensionalen zyklischen Funktion ist $Y_{\frac{1}{8}\cdot\frac{1}{3}}\, Y_{\frac{1}{8}\cdot\frac{2}{3}}$. Zur Darstellung desselben bilden wir die Kombinationen des ersten Restes 1 von $Y_{\frac{1}{8}\cdot\frac{1}{3}}$ mit allen Resten von $Y_{\frac{1}{8}\cdot\frac{2}{3}}$; Diess giebt die drei Zahlen 3, 17, 56, welche den Horizontalreihen 4, 6, 5 und in diesen den Partialreihen $Y_{\frac{4}{8}\cdot\frac{1}{3}}$, $Y_{\frac{6}{8}\cdot\frac{3}{3}}$, $Y_{\frac{5}{8}\cdot\frac{2}{3}}$ angehören. Durch horizontale Verschiebung dieser Kombinationen um die Breite einer Partialreihe, also um drei Stellen, füllen sich die zuletzt genannten drei Partialreihen und man erhält statt Gl. (1) in Nr. 7

$$Y_{\frac{1}{8}\cdot\frac{1}{3}}\, Y_{\frac{1}{8}\cdot\frac{2}{3}} = Y_{\frac{4}{8}\cdot\frac{1}{3}} + Y_{\frac{6}{8}\cdot\frac{3}{3}} + Y_{\frac{5}{8}\cdot\frac{2}{3}}$$

Hieraus ergeben sich für die beiden folgenden Glieder der zweidimensionalen Funktion durch horizontale Verschiebung

$$Y_{\frac{1}{8}\cdot\frac{2}{3}}\, Y_{\frac{1}{8}\cdot\frac{3}{3}} = Y_{\frac{4}{8}\cdot\frac{2}{3}} + Y_{\frac{6}{8}\cdot\frac{1}{3}} + Y_{\frac{5}{8}\cdot\frac{3}{3}}$$

$$Y_{\frac{1}{8}\cdot\frac{3}{3}}\, Y_{\frac{1}{8}\cdot\frac{1}{3}} = Y_{\frac{4}{8}\cdot\frac{3}{3}} + Y_{\frac{6}{8}\cdot\frac{2}{3}} + Y_{\frac{5}{8}\cdot\frac{1}{3}}$$

und demgemäss für die ganze zweidimensionale Funktion nach Gl. (3)

$$Y_{\frac{1}{8}\cdot\frac{1}{3}}\, Y_{\frac{1}{8}\cdot\frac{2}{3}} + Y_{\frac{1}{8}\cdot\frac{2}{3}}\, Y_{\frac{1}{8}\cdot\frac{3}{3}} + Y_{\frac{1}{8}\cdot\frac{3}{3}}\, Y_{\frac{1}{8}\cdot\frac{1}{3}} = Y_{\frac{4}{8}} + Y_{\frac{6}{8}} + Y_{\frac{5}{8}}$$

Die Zerlegung der übrigen Horizontalreihen erfordert eine vertikale Verschiebung, deren Gesetz durch die ersten Exponenten der Horizontalreihen der Exponententafel E hervortritt. Bezeichnen wir also die

1., 2., 3., 4., 5., 6., 7., 8. Reihe

mit

0 4 2 6 1 5 3 7

so erhalten wir statt der letzten und der daraus abgeleiteten Formeln, indem wir aus der geordneten Grundtafel Y in die erste Grundtafel G übertreten und demgemäss auch G für Y schreiben,

$$G_{\frac{0}{8}\cdot\frac{1}{3}}\,G_{\frac{0}{8}\cdot\frac{2}{3}} + G_{\frac{0}{8}\cdot\frac{2}{3}}\,G_{\frac{0}{8}\cdot\frac{3}{3}} + G_{\frac{0}{8}\cdot\frac{3}{3}}\,G_{\frac{0}{8}\cdot\frac{1}{3}} = G_{\frac{6}{8}} + G_{\frac{5}{8}} + G_{\frac{1}{8}}$$
$$G_{\frac{1}{8}\cdot\frac{1}{3}}\,G_{\frac{1}{8}\cdot\frac{2}{3}} + G_{\frac{1}{8}\cdot\frac{2}{3}}\,G_{\frac{1}{8}\cdot\frac{3}{3}} + G_{\frac{1}{8}\cdot\frac{3}{3}}\,G_{\frac{1}{8}\cdot\frac{1}{3}} = G_{\frac{7}{8}} + G_{\frac{6}{8}} + G_{\frac{2}{8}}$$
$$G_{\frac{2}{8}\cdot\frac{1}{3}}\,G_{\frac{2}{8}\cdot\frac{2}{3}} + G_{\frac{2}{8}\cdot\frac{2}{3}}\,G_{\frac{2}{8}\cdot\frac{3}{3}} + G_{\frac{2}{8}\cdot\frac{3}{3}}\,G_{\frac{2}{8}\cdot\frac{1}{3}} = G_{\frac{0}{8}} + G_{\frac{7}{8}} + G_{\frac{3}{8}}$$
$$G_{\frac{3}{8}\cdot\frac{1}{3}}\,G_{\frac{3}{8}\cdot\frac{2}{3}} + G_{\frac{3}{8}\cdot\frac{2}{3}}\,G_{\frac{3}{8}\cdot\frac{3}{3}} + G_{\frac{3}{8}\cdot\frac{3}{3}}\,G_{\frac{3}{8}\cdot\frac{1}{3}} = G_{\frac{1}{8}} + G_{\frac{0}{8}} + G_{\frac{4}{8}}$$
$$G_{\frac{4}{8}\cdot\frac{1}{3}}\,G_{\frac{4}{8}\cdot\frac{2}{3}} + G_{\frac{4}{8}\cdot\frac{2}{3}}\,G_{\frac{4}{8}\cdot\frac{3}{3}} + G_{\frac{4}{8}\cdot\frac{3}{3}}\,G_{\frac{4}{8}\cdot\frac{1}{3}} = G_{\frac{2}{8}} + G_{\frac{1}{8}} + G_{\frac{5}{8}}$$
$$G_{\frac{5}{8}\cdot\frac{1}{3}}\,G_{\frac{5}{8}\cdot\frac{2}{3}} + G_{\frac{5}{8}\cdot\frac{2}{3}}\,G_{\frac{5}{8}\cdot\frac{3}{3}} + G_{\frac{5}{8}\cdot\frac{3}{3}}\,G_{\frac{5}{8}\cdot\frac{1}{3}} = G_{\frac{3}{8}} + G_{\frac{2}{8}} + G_{\frac{6}{8}}$$
$$G_{\frac{6}{8}\cdot\frac{1}{3}}\,G_{\frac{6}{8}\cdot\frac{2}{3}} + G_{\frac{6}{8}\cdot\frac{2}{3}}\,G_{\frac{6}{8}\cdot\frac{3}{3}} + G_{\frac{6}{8}\cdot\frac{3}{3}}\,G_{\frac{6}{8}\cdot\frac{1}{3}} = G_{\frac{4}{8}} + G_{\frac{3}{8}} + G_{\frac{7}{8}}$$
$$G_{\frac{7}{8}\cdot\frac{1}{3}}\,G_{\frac{7}{8}\cdot\frac{2}{3}} + G_{\frac{7}{8}\cdot\frac{2}{3}}\,G_{\frac{7}{8}\cdot\frac{3}{3}} + G_{\frac{7}{8}\cdot\frac{3}{3}}\,G_{\frac{7}{8}\cdot\frac{1}{3}} = G_{\frac{5}{8}} + G_{\frac{4}{8}} + G_{\frac{0}{8}}$$

Überträgt man diese Formeln von der Tafel G auf die Tafel Y, so werden dieselben

$$Y_{\frac{1}{8}\cdot\frac{1}{3}}\,Y_{\frac{1}{8}\cdot\frac{2}{3}} + Y_{\frac{1}{8}\cdot\frac{2}{3}}\,Y_{\frac{1}{8}\cdot\frac{3}{3}} + Y_{\frac{1}{8}\cdot\frac{3}{3}}\,Y_{\frac{1}{8}\cdot\frac{1}{3}} = Y_{\frac{4}{8}} + Y_{\frac{6}{8}} + Y_{\frac{5}{8}}$$
$$Y_{\frac{5}{8}\cdot\frac{1}{3}}\,Y_{\frac{5}{8}\cdot\frac{2}{3}} + Y_{\frac{5}{8}\cdot\frac{2}{3}}\,Y_{\frac{5}{8}\cdot\frac{3}{3}} + Y_{\frac{5}{8}\cdot\frac{3}{3}}\,Y_{\frac{5}{8}\cdot\frac{1}{3}} = Y_{\frac{8}{8}} + Y_{\frac{4}{8}} + Y_{\frac{3}{8}}$$
$$Y_{\frac{3}{8}\cdot\frac{1}{3}}\,Y_{\frac{3}{8}\cdot\frac{2}{3}} + Y_{\frac{3}{8}\cdot\frac{2}{3}}\,Y_{\frac{3}{8}\cdot\frac{3}{3}} + Y_{\frac{3}{8}\cdot\frac{3}{3}}\,Y_{\frac{3}{8}\cdot\frac{1}{3}} = Y_{\frac{1}{8}} + Y_{\frac{8}{8}} + Y_{\frac{7}{8}}$$
$$Y_{\frac{7}{8}\cdot\frac{1}{3}}\,Y_{\frac{7}{8}\cdot\frac{2}{3}} + Y_{\frac{7}{8}\cdot\frac{2}{3}}\,Y_{\frac{7}{8}\cdot\frac{3}{3}} + Y_{\frac{7}{8}\cdot\frac{3}{3}}\,Y_{\frac{7}{8}\cdot\frac{1}{3}} = Y_{\frac{5}{8}} + Y_{\frac{1}{8}} + Y_{\frac{2}{8}}$$
$$Y_{\frac{2}{8}\cdot\frac{1}{3}}\,Y_{\frac{2}{8}\cdot\frac{2}{3}} + Y_{\frac{2}{8}\cdot\frac{2}{3}}\,Y_{\frac{2}{8}\cdot\frac{3}{3}} + Y_{\frac{2}{8}\cdot\frac{3}{3}}\,Y_{\frac{2}{8}\cdot\frac{1}{3}} = Y_{\frac{3}{8}} + Y_{\frac{5}{8}} + Y_{\frac{6}{8}}$$
$$Y_{\frac{6}{8}\cdot\frac{1}{3}}\,Y_{\frac{6}{8}\cdot\frac{2}{3}} + Y_{\frac{6}{8}\cdot\frac{2}{3}}\,Y_{\frac{6}{8}\cdot\frac{3}{3}} + Y_{\frac{6}{8}\cdot\frac{3}{3}}\,Y_{\frac{6}{8}\cdot\frac{1}{3}} = Y_{\frac{7}{8}} + Y_{\frac{3}{8}} + Y_{\frac{4}{8}}$$
$$Y_{\frac{4}{8}\cdot\frac{1}{3}}\,Y_{\frac{4}{8}\cdot\frac{2}{3}} + Y_{\frac{4}{8}\cdot\frac{2}{3}}\,Y_{\frac{4}{8}\cdot\frac{3}{3}} + Y_{\frac{4}{8}\cdot\frac{3}{3}}\,Y_{\frac{4}{8}\cdot\frac{1}{3}} = Y_{\frac{2}{8}} + Y_{\frac{7}{8}} + Y_{\frac{8}{8}}$$
$$Y_{\frac{8}{8}\cdot\frac{1}{3}}\,Y_{\frac{8}{8}\cdot\frac{2}{3}} + Y_{\frac{8}{8}\cdot\frac{2}{3}}\,Y_{\frac{8}{8}\cdot\frac{3}{3}} + Y_{\frac{8}{8}\cdot\frac{3}{3}}\,Y_{\frac{8}{8}\cdot\frac{1}{3}} = Y_{\frac{6}{8}} + Y_{\frac{2}{8}} + Y_{\frac{1}{8}}$$

Die dreidimensionale Funktion von $Y_{\frac{1}{8}\cdot\frac{1}{3}}$, $Y_{\frac{1}{8}\cdot\frac{2}{3}}$, $Y_{\frac{1}{8}\cdot\frac{3}{3}}$ besteht aus dem einzigen Gliede $Y_{\frac{1}{8}\cdot\frac{1}{3}}\,Y_{\frac{1}{8}\cdot\frac{2}{3}}\,Y_{\frac{1}{8}\cdot\frac{3}{3}}$. Nachdem die zweidimensionale Kombination $Y_{\frac{1}{8}\cdot\frac{2}{3}}\,Y_{\frac{1}{8}\cdot\frac{3}{3}}$ schon gebildet und dafür der Werth $Y_{\frac{4}{8}\cdot\frac{2}{3}} + Y_{\frac{6}{8}\cdot\frac{1}{3}} + Y_{\frac{5}{8}\cdot\frac{3}{3}}$ gefunden ist, kömmt es nur noch

darauf an, alle in dem letzteren Werthe enthaltenen Reste 6, 48, 19, 59, 34, 53, 20, 14, 39 mit dem ersten Reste 1 der Gruppe $Y_{\frac{1}{8}\cdot\frac{1}{3}}$ zu kombiniren. Diess giebt die Reste 7, 49, 20, 60, 35, 54, 21, 15 40, wovon je 3 den Horizontalreihen 3, 5, 8 und zwar den verschiedenen Dritteln derselben angehören. Durch zweimalige Horizontalverschiebung füllen sich diese drei Horizontalreihen und man erhält

$$Y_{\frac{1}{8}\cdot\frac{1}{3}}\ Y_{\frac{1}{8}\cdot\frac{2}{3}}\ Y_{\frac{1}{8}\cdot\frac{3}{3}} = Y_{\frac{3}{8}} + Y_{\frac{5}{8}} + Y_{\frac{8}{8}}$$

oder mit Übertragung auf die Tafel G unter Bezeichnung der Zeiger durch die Exponenten der Tafel E

$$G_{\frac{0}{8}\cdot\frac{1}{3}}\ G_{\frac{0}{8}\cdot\frac{2}{3}}\ G_{\frac{0}{8}\cdot\frac{3}{3}} = G_{\frac{2}{8}} + G_{\frac{1}{8}} + G_{\frac{7}{8}}$$

Hieraus folgt für die folgenden dreidimensionalen Funktionen

$$G_{\frac{1}{8}\cdot\frac{1}{3}}\ G_{\frac{1}{8}\cdot\frac{2}{3}}\ G_{\frac{1}{8}\cdot\frac{3}{3}} = G_{\frac{3}{8}} + G_{\frac{2}{8}} + G_{\frac{0}{8}}$$

$$G_{\frac{2}{8}\cdot\frac{1}{3}}\ G_{\frac{2}{8}\cdot\frac{2}{3}}\ G_{\frac{2}{8}\cdot\frac{3}{3}} = G_{\frac{4}{8}} + G_{\frac{3}{8}} + G_{\frac{1}{8}}$$

u. s. w. Bei Rückkehr zur Tafel Y werden die letzteren Formeln

$$Y_{\frac{5}{8}\cdot\frac{1}{3}}\ Y_{\frac{5}{8}\cdot\frac{2}{3}}\ Y_{\frac{5}{8}\cdot\frac{3}{3}} = Y_{\frac{7}{8}} + Y_{\frac{3}{8}} + Y_{\frac{1}{8}}$$

$$Y_{\frac{3}{8}\cdot\frac{1}{3}}\ Y_{\frac{3}{8}\cdot\frac{2}{3}}\ Y_{\frac{3}{8}\cdot\frac{3}{3}} = Y_{\frac{2}{8}} + Y_{\frac{7}{8}} + Y_{\frac{5}{8}}$$

u. s. w.

Schliesslich handelt es sich um die Zerlegung der Gruppen $Y_{\frac{1}{8}\cdot\frac{1}{3}}$ etc. in ihre drei Elemente $Y_{\frac{1}{8}\cdot\frac{1}{9}}$, $Y_{\frac{1}{8}\cdot\frac{2}{9}}$, $Y_{\frac{1}{8}\cdot\frac{3}{9}}$ etc. Die eindimensionale Funktion der ersten Gruppe ist

$$Y_{\frac{1}{8}\cdot\frac{1}{9}} + Y_{\frac{1}{8}\cdot\frac{2}{9}} + Y_{\frac{1}{8}\cdot\frac{3}{9}} = Y_{\frac{1}{8}\cdot\frac{1}{3}}$$

Die zweidimensionale Funktion ist, indem wir das leicht zu überblickende Resultat sogleich daneben setzen,

$$Y_{\frac{1}{8}\cdot\frac{1}{9}}\ Y_{\frac{1}{8}\cdot\frac{2}{9}} + Y_{\frac{1}{8}\cdot\frac{2}{9}}\ Y_{\frac{1}{8}\cdot\frac{3}{9}} + Y_{\frac{1}{8}\cdot\frac{3}{9}}\ Y_{\frac{1}{8}\cdot\frac{1}{9}} = 9 + 72 + 65 = Y_{\frac{2}{8}\cdot\frac{2}{3}}$$

Durch horizontale Verschiebung ergiebt sich hieraus

$$Y_{\frac{1}{8}\cdot\frac{4}{9}}\ Y_{\frac{1}{8}\cdot\frac{5}{9}} + Y_{\frac{1}{8}\cdot\frac{5}{9}}\ Y_{\frac{1}{8}\cdot\frac{6}{9}} + Y_{\frac{1}{8}\cdot\frac{6}{9}}\ Y_{\frac{1}{8}\cdot\frac{4}{9}} = Y_{\frac{2}{8}\cdot\frac{3}{3}}$$

$$Y_{\frac{1}{8}\cdot\frac{7}{9}}\ Y_{\frac{1}{8}\cdot\frac{8}{9}} + Y_{\frac{1}{8}\cdot\frac{8}{9}}\ Y_{\frac{1}{8}\cdot\frac{9}{9}} + Y_{\frac{1}{8}\cdot\frac{9}{9}}\ Y_{\frac{1}{8}\cdot\frac{7}{9}} = Y_{\frac{2}{8}\cdot\frac{1}{3}}$$

Behuf der vertikalen Verschiebung übertragen wir die erste dieser drei Formeln auf die Tafel G, schreiben also mit Bezug auf die Exponenten der Tafel E für die Zerlegung des ersten Drittels jeder Horizontalreihe

$$G_{\frac{0}{8}\cdot\frac{1}{9}}\, G_{\frac{0}{8}\cdot\frac{2}{9}} + G_{\frac{0}{8}\cdot\frac{2}{9}}\, G_{\frac{0}{8}\cdot\frac{3}{9}} + G_{\frac{0}{8}\cdot\frac{3}{9}}\, G_{\frac{0}{8}\cdot\frac{1}{9}} = G_{\frac{4}{8}\cdot\frac{2}{3}}$$

Hieraus folgt bei vertikaler Verschiebung

$$G_{\frac{1}{8}\cdot\frac{1}{9}}\, G_{\frac{1}{8}\cdot\frac{2}{9}} + G_{\frac{1}{8}\cdot\frac{2}{9}}\, G_{\frac{1}{8}\cdot\frac{3}{9}} + G_{\frac{1}{8}\cdot\frac{3}{9}}\, G_{\frac{1}{8}\cdot\frac{1}{9}} = G_{\frac{5}{8}\cdot\frac{2}{3}}$$

$$G_{\frac{2}{8}\cdot\frac{1}{9}}\, G_{\frac{2}{8}\cdot\frac{2}{9}} + G_{\frac{2}{8}\cdot\frac{2}{9}}\, G_{\frac{2}{8}\cdot\frac{3}{9}} + G_{\frac{2}{8}\cdot\frac{3}{9}}\, G_{\frac{2}{8}\cdot\frac{1}{9}} = G_{\frac{6}{8}\cdot\frac{2}{3}}$$

u. s. w. und wenn man diese Formeln wieder auf die Tafel Y überträgt,

$$Y_{\frac{5}{8}\cdot\frac{1}{9}}\, Y_{\frac{5}{8}\cdot\frac{2}{9}} + Y_{\frac{5}{8}\cdot\frac{2}{9}}\, Y_{\frac{5}{8}\cdot\frac{3}{9}} + Y_{\frac{5}{8}\cdot\frac{3}{9}}\, Y_{\frac{5}{8}\cdot\frac{1}{9}} = Y_{\frac{6}{8}\cdot\frac{2}{3}}$$

$$Y_{\frac{3}{8}\cdot\frac{1}{9}}\, Y_{\frac{3}{8}\cdot\frac{2}{9}} + Y_{\frac{3}{8}\cdot\frac{2}{9}}\, Y_{\frac{3}{8}\cdot\frac{3}{9}} + Y_{\frac{3}{8}\cdot\frac{3}{9}}\, Y_{\frac{3}{8}\cdot\frac{1}{9}} = Y_{\frac{4}{8}\cdot\frac{2}{3}}$$

u. s. w. Für die Zerlegung des zweiten und des dritten Drittels jeder Horizontalreihe verändert sich auf der rechten Seite dieser Gleichungen der Bruch $\frac{2}{3}$ des Zeigers resp. in $\frac{3}{3}$ und $\frac{1}{3}$.

10) Wenn 2 eine primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \bmod p$ ist, was unter Anderem für die Primzahlen $p = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67$ (jedoch nicht für die dazwischen liegenden Primzahlen 7, 17, 23, 31, 41, 43, 47) der Fall ist; so reduzirt sich die Grundtafel auf eine einzige Horizontalreihe.

11) In der Anwendung der vorstehenden Periodengleichungen auf die Auflösung der Gleichung $x^p - 1 = 0$ oder

$$x^{p-1} + x^{p-2} + \ldots + x^2 + x = -1$$

ist in jenen Gleichungen $Y = -1$ zu setzen.

Was den Werth für jeden in jenen Formeln erscheinenden Nullrest betrifft; so ist derselbe offenbar, da er einen Exponenten von x vertritt, gleich 1 zu setzen, da x^0, welchen Werth auch x haben möge, stets $= 1$ ist. Hiernach ist $Y(0) = p - 1$ und $Y_{\frac{1}{r}}(0) = \frac{p-1}{r}$, $Y_{\frac{1}{r}\cdot\frac{1}{s}}(0) = \frac{p-1}{rs}$ zu setzen. In dem Beispiele in Nr. 9 würde $Y_{\frac{1}{8}}(0) = \frac{72}{8} = 9$ sein.

Die Auflösung der gegebenen Gleichung vom Grade p wird vermittelst der obigen symmetrischen Funktionen auf die Auflösung von Gleichungen zurückgeführt, deren Grade Faktoren von $p - 1$ sind. Zur

vollständigen Auflösung reicht indess die Kenntniss der Wurzeln dieser niedrigeren Grade nur in dem in §. 1 bis 3 behandelten, sowie in einigen späterhin (§. 7 Nr. 11) zu bezeichnenden speziellen Fällen aus: im Allgemeinen ist sie nicht ausreichend, es muss vielmehr auch die Reihenfolge bekannt sein, in welcher die Wurzeln der einen Zerlegung bei der nächst folgenden Zerlegung zu nehmen sind. Diese bis jetzt noch ungelös'te Aufgabe hinsichtlich der Anordnung der Wurzeln werden wir in §. 7 erledigen.

§. 6. Independente Formeln.

1) Wenn es sich um einen beliebigen Werth der Primzahl p und um eine vollständige Auflösung der Gleichung $x^p - 1 = 0$ handelt, dürfte es kaum ein einfacheres und kürzeres Verfahren, als das in den vorstehenden Nummern entwickelte geben. Dasselbe ist von den Faktoren der Zahl $p - 1$ unabhängig und führt durch die einfachsten Operationen auf einem rekursorischen Wege zur Kenntniss aller erforderlichen symmetrischen Funktionen f_1, f_2, f_3 etc. (resp. deren primitiven zyklischen Reihen). Für bestimmte Faktoren der Zahl $p - 1$ können natürlich auch independente Formeln für diese Funktionen und demzufolge auch für die Gleichungen von der Form

$$x^n - f_1 \cdot x^{n-1} + f_2 \cdot x^{n-2} - f_3\, x^{n-3} + \text{etc.} = 0$$

aufgestellt werden, wozu die Formeln in Nr. 6 Gelegenheit bieten. Die Ausdrücke in Gl. (6), (7), (8) für die Summe σ der Koeffizienten sind schon solche independente Formeln: einige andere ergeben sich durch folgende Betrachtung.

Man kann jeden Primfaktor r von $p - 1 = s\,r$ als den ersten annehmen und danach die Grundtafel in vertikaler Richtung ordnen, sodass dieselbe in r Horizontalstreifen P_1, P_2 . . . P_r von je n Resten zerfällt. Insofern man lediglich eine Beziehung zwischen den Gruppen P und der Gesammttafel Y sucht, kann man diese Tafel so ordnen, dass ihre Reste der Exponententafel

P_1	0	r	$2r$	. . .	$(s-1)\,r$
P_2	1	$r+1$	$2r+1$		$(s-1)\,r+1$
P_3	2	$r+2$	$2r+2$		$(s-1)\,r+1$
.	.	.	.		.
.	.	.	.		.
.	.	.	.		.
P_r	$r-1$	$2r-1$	$3r-1$		$sr-1$

entsprechen, worin jedes P als eine Horizontalreihe von n Elementen

erscheint. Bei der gemachten Beschränkung braucht r nicht nothwendig eine Primzahl zu sein.

Für manche Zwecke ist es wichtig, die Stelle gewisser Reste zu kennen. Der erste Rest der Tafel ist stets 1. Die Stelle des Restes $p-1$ oder sein Exponent α ergiebt sich durch die Erwägung, dass $a^\alpha \equiv p-1 \equiv -1$, also $a^{2\alpha} \equiv 1$ mithin, da 2α nicht $= 0$ sein kann (indem der Exponent 0 dem ersten Reste 1 der Tafel angehört), $2\alpha = p-1$, also $\alpha = \frac{p-1}{2} = \frac{sr}{2}$ sein muss. Ist s paar; so gehört $\alpha = \frac{s}{2} . r$ der ersten Horizontalreihe P_1 an: ist dagegen s unpaar $= 2n+1$, also r unfehlbar paar; so gehört $\alpha = nr + \frac{r}{2}$ der Horizontalreihe vom Zeiger $\frac{r}{2}+1$, also der Reihe $P_{\frac{r}{2}+1}$ an.

Die Summe der beiden Reste 1 und $p-1$ liefert einen Nullrest. Aus $a^0 + a^{\frac{p-1}{2}} \equiv 1 - 1 \equiv 0$ folgt aber auch für jeden Werth von β die Kongruenz

$$a^\beta \left(a^0 + a^{\frac{p-1}{2}}\right) = a^\beta + a^{\frac{p-1}{2}+\beta} \equiv 0$$

Zwei Reste, deren Exponenten sich um den Betrag $\frac{p-1}{2}$ unterscheiden, liefern also durch Summirung einen Nullrest, sonst aber keine anderen. Wenn s paar ist, liegen solche zwei Reste stets in einundderselben Reihe P; Kombinationen zweier verschiedenen Horizontalreihen können also dann keine Nullreste ergeben. Wenn s unpaar ist, liegen zwei Reste der gedachten Art immer in zwei verschiedenen Reihen P, deren Zeiger sich um den Betrag $\frac{r}{2}$ unterscheiden, also in den beiden Reihen von den Zeigern 1 und $\frac{r}{2}+1$, ferner 2 und $\frac{r}{2}+2$, ferner 3 und $\frac{r}{2}+3$ u. s. w.

Allgemein, leuchtet ein, dass wenn γ der Exponent irgend eines Restes c, also $a^\gamma \equiv c$ ist, der Exponent $\gamma + \frac{p-1}{2}$ dem Reste $p-c$ entsprechen wird, da $a^{\gamma+\frac{p-1}{2}} = a^\gamma a^{\frac{p-1}{2}} \equiv -a^\gamma \equiv -c$ ist, sodass die Summe der zu den Exponenten γ und $\gamma + \frac{p-1}{2}$ gehörigen Reste immer einen Nullrest liefert.

Je zwei Reste c und $p-c$ oder c und $-c$ nehmen hiernach Stellen ein, welche sich wie die Stellen der beiden Reste 1 und $p-1$ oder 1 und -1 unterscheiden. Kennt man die Stelle des einen; so ergiebt sich daraus die Stelle des anderen. Zwei solche Reste liegen, wenn s paar ist, stets in denselben Horizontalreihen P, und wenn s unpaar ist, in Horizontalreihen P, deren Zeiger sich um $\frac{r}{2}$ unterscheiden. Die Grundtafel zerfällt hiernach in zwei Hälften, eine linke und eine rechte, von

welchen die rechte diejenigen Reste $p - c$ oder $-c$ enthält, welche die negativen Werthe der Reste der linken Hälfte in derselben Reihenfolge enthält.

Setzt man an die Stelle eines Restes c der rechten Hälfte den äquivalenten negativen Werth $-(p-c)$; so nimmt die Grundtafel der Reste, welche der letzten Tafel der Exponenten entspricht, jenachdem s paar oder unpaar ist, folgende Gestalt I oder II der positiven und negativen Reste an, wobei wir statt der Reste die Potenzen von a gesetzt haben, welchen sie kongruent sind.

I., für ein paares $s = 2n$ und ein paares oder unpaares r

P_1	a^0	a^r	a^{2r}	$\dots$	$a^{(n-1)r}$	$-a^0$	$-a^r$	$-a^{2r}$	$\dots -a^{(n-1)r}$
P_2	a^1	a^{r+1}	a^{2r+1}	$\dots$	$a^{(n-1)r+1}$	$-a^1$	$-a^{r+1}$	$-a^{2r+1}$	$-a^{(n-1)r+1}$
P_3	a^2	a^{r+2}	a^{2r+2}	$\dots$	$a^{(n-1)r+2}$	$-a^2$	$-a^{r+2}$	$-a^{2r+1}$	$-a^{(n-1)r+2}$
	.					.			
	.					.			
	.					.			
P_r	a^{r-1}	a^{2r-1}	a^{3r-1}	$\dots$	a^{nr-1}	$-a^{r-1}$	$-a^{2r-1}$	$-a^{3r-1}$	$-a^{nr-1}$

II., für ein unpaares s, welches ein paares $r = 2m$ bedingt,

P_1	a^0	a^r	a^{2r}	$\dots$	$a^{(s-3)m}$	$a^{(s-1)m}$	$-a^m$	$-a^{3m}$	$\dots -a^{(s-2)m}$
P_2	a^1	a^{r+1}	a^{2r+1}		$a^{(s-3)m+1}$	$a^{(s-1)m+1}$	$-a^{m+1}$	$-a^{3m+1}$	$-a^{(s-2)m+1}$
	.						.		
	.						.		
	.						.		
P_m	a^{m-1}	a^{3m-1}	a^{5m-1}		$a^{(s-2)m-1}$	a^{sm-1}	$-a^{r-1}$	$-a^{2r-1}$	$-a^{(s-1)m-1}$
P_{m+1}	a^m	a^{3m}	a^{5m}		$a^{(s-2)m}$	$-a^0$	$-a^r$	$-a^{2r}$	$-a^{(s-1)m}$
P_{m+2}	a^{m+1}	a^{3m+1}	a^{5m+1}		$a^{(s-2)m+1}$	$-a^1$	$-a^{r+1}$	$-a^{2r+1}$	$-a^{(s-1)m+1}$
	.					.			
	.					.			
	.					.			
P_r	a^{r-1}	a^{2r-1}	a^{3r-1}		$a^{(s-1)m-1}$	$-a^{m-1}$	$-a^{3m-1}$	$-a^{5m-1}$	$-a^{sm-1}$

2) Die Kongruenz $a^x + c \equiv a^y$ zieht die Kongruenz $-a^y + c \equiv -a^x$ oder, indem man $-1 \equiv a^{\frac{p-1}{2}}$ setzt, die Kongruenz $a^{y+\frac{p-1}{2}} + c \equiv a^{x+\frac{p-1}{2}}$ nach sich. Der Rest von a^x gehört der Horizontalreihe P_{x+1} oder, wenn $x+1$ grösser als r ist, der Reihe P_{x+1-vr} an; ebenso gehört der Rest von a^y der Reihe P_{y+1} resp. P_{y+1-vr}, ferner der Rest von $a^{x+\frac{p-1}{2}}$ und von $a^{y+\frac{p-1}{2}}$ den Reihen $P_{x+1+\frac{p-1}{2}-vr}$ und $P_{y+1+\frac{p-1}{2}-vr}$ an. Ist in dem Werthe $p - 1 = sr$ der Faktor s paar $= 2n$; so ist $\frac{p-1}{2} = nr$ ein Vielfaches von r und demzufolge kann in den Zeigern von P das Glied $\frac{p-1}{2}$ unterdrückt werden. Ist dagegen s unpaar und

daher r paar $= 2m$, also $\frac{p-1}{2} = \frac{s-1}{2} r + \frac{r}{2}$; so kann man in den Zeigern von P das Glied $\frac{s-1}{2} r$ unterdrücken oder für $\frac{p-1}{2}$ das Glied $\frac{r}{2} = m$ setzen.

Wenn hiernach die Addition der Zahl c zu einem Reste der Reihe P_α eine Zahl der Reihe P_β liefert; so liefert im ersten Fall, für ein paares s, die Addition derselben Zahl c zu einem Reste der Reihe P_β eine Zahl der Reihe P_α, im zweiten Fall dagegen, für ein unpaares s, liefert die Addition der Zahl c zu einem Reste der Reihe $P_{\beta+m}$ eine Zahl der Reihe $P_{\alpha+m}$.

Dieser Satz gilt für jeden Werth von c, also auch für $c = 1$, welche Zahl den ersten Rest der ersten Reihe P_1 bildet. So oft mithin in der Kombination $P_1\ P_\alpha$ der Reihe P_1 mit einer anderen Reihe P_α die Summe des ersten Restes 1 mit einem Reste von P_α eine Zahl der Reihe P_β liefert, ebenso oft liefert im ersten Falle in der Kombination $P_1\ P_\beta$ die Summe des ersten Restes 1 mit einem Reste von P_β eine Zahl der Reihe P_α, im zweiten Falle dagegen gilt Diess von den Kombinationen $P_1\ P_{\beta+m}$ und $P_1\ P_{\alpha+m}$, indem man für die Zeiger $\alpha + m$ und $\beta + m$ die kleinsten positiven Werthe der Grössen $\alpha + m - vr$ und $\beta + m - vr$ annimmt. Nach Gl. (1) hat eine Kombination mehrerer Reihen P die Form

$$P_1\ P_\alpha = \pi_0\ P_0 + \pi_1\ P_1 + \pi_2\ P_2 + \ldots\ \pi_\alpha\ P_\alpha \ldots\ \pi_\beta\ P_\beta \ldots\ \pi_\gamma\ P_\gamma$$

und ähnlich ist

$$P_1\ P_\beta = \varrho_0\ P_0 + \varrho_1\ P_1 + \varrho_2\ P_2 + \ldots\ \varrho_\alpha\ P_\alpha \ldots$$

Im ersten Falle, für ein paares s, ist mithin der Koeffizient $\pi_\beta = \varrho_\alpha$.

Setzt man im zweiten Falle, für ein unpaares s,

$$P_1\ P_{\beta+m} = \varrho_0\ P_0 + \varrho_1\ P_1 + \varrho_2\ P_2 + \ldots + \varrho_{\alpha+m}\ P_{\alpha+m} + \ldots$$

so ist der Koeffizient $\pi_\beta = \varrho_{\alpha+m}$.

Nimmt man $\alpha = 1$; sodass

$$P_1\ P_1 = P_1^{\,2} = \pi_0\ P_0 + \pi_1\ P_1 + \pi_2\ P_2 + \ldots\ \pi_\beta\ P_\beta \ldots$$

ist; so hat man im ersten Fall $\pi_\beta = \varrho_1$ und im zweiten Fall $\pi_\beta = \varrho_{1+m}$.

Für einen beliebigen Werth von c gelten die vorstehenden Formeln, indem man auf der linken Seite statt P_1 diejenige Reihe P_γ substituirt, welcher der Rest c angehört.

3) Aus der Kongruenz $a^x + 1 = a^y$ folgt durch Multiplikation mit a^{r-x} die Kongruenz $a^r + a^{r-x} = a^{r+y-x}$. In der ersten Kongruenz gehören die Reste von 1, a^x, a^y resp. den Reihen P_1, P_{x+1}, P_{y+1}, in der zweiten Kongruenz gehören die Reste von a^r, a^{r-x}, a^{r+y-x} resp. den Reihen P_{r+1}, P_{r-x+1}, $P_{r+y-x+1}$ an, und diese Reihen sind identisch bezw. mit den Reihen P_1, P_{r-x+1}, P_{y-x+1}. So oft also die Kombination $P_1\ P_{x+1}$ einen Rest aus der Reihe P_{y+1} liefert, ebenso oft liefert die Kombination $P_1\ P_{r-x+1}$ einen Rest aus der Reihe P_{y-x+1}. Setzt man $x + 1 = \alpha$ und $y + 1 = \beta$; so folgt, dass so oft $P_1\ P_\alpha$ einen Rest der Reihe P_β enthält, $P_1\ P_{r-\alpha+2}$ einen Rest der Reihe $P_{\beta-\alpha+1}$ enthalten

wird. Dieser Satz gilt für beide obigen Fälle, nämlich für ein gerades und ungerades s.

4) Bezeichnet man die Koeffizienten von $P_0, P_1, P_2, P_3 \ldots$ in der Kombination von P_1 mit irgend einer Reihe P_x, also in der Kombination $P_1 P_x$ bezw. mit $x_0, x_1, x_2, x_3 \ldots$; so ist die Beziehung in Nr. 2

$$(9) \qquad \begin{cases} \text{für ein paares } s & u_\beta = \beta_\alpha \\ \text{für ein unpaares } s & u_\beta = (\beta + m)_{\alpha+m} \end{cases}$$

und die Beziehung in Nr. 3 ist für jedes beliebige s

$$(10) \qquad u_\beta = (r - \alpha + 2)_{\beta-\alpha+1}$$

Wenn $\alpha \geq \beta + 1$, also $\beta - \alpha + 1$ negativ ist, hat man dafür in der letzten Gleichung $r + \beta - \alpha + 1$ zu setzen.

Die Gleichungen (9) und (10) stimmen (abgesehen von der Bezeichnung) mit den Formeln (6) und (5) überein, welche von Kummer in der Abhandlung über die Zerlegung der Wurzeln der Einheit in Crelle's Journal Band 35 S. 329 auf einem anderen Wege dargestellt und von Bachmann in der Lehre von der Kreistheilung auf S. 202 u. 203 reproduzirt sind. Der von Kummer eingeschlagene Weg ist zwar etwas kürzer, als der unserige, letzterer ist jedoch anschaulicher und führt zugleich die im vorhergehenden Paragraphen dargestellte konkrete Lösung jedes speziellen Falles unmittelbar und mit den einfachsten Mitteln herbei.

5) Mit Hülfe der hier und in §. 5 aufgestellten Formeln lassen sich die Werthe aller symmetrischen Funktionen der Grössen P leicht bestimmen. Wir setzen zu dem Ende

$$P_1 P_1 = 1_0 P_0 + 1_1 P_1 + 1_2 P_2 + 1_3 P_3 + \ldots + 1_r P_r$$

und gehen zunächst darauf aus, die Werthe von

$$P_1 P_2 = 2_0 P_0 + 2_1 P_1 + 2_2 P_2 + 2_3 P_3 + \ldots + 2_r P_r$$
$$P_1 P_3 = 3_0 P_0 + 3_1 P_1 + 3_2 P_2 + 3_3 P_3 + \ldots + 3_r P_r$$
$$\vdots$$
$$P_1 P_r = r_0 P_0 + r_1 P_1 + r_2 P_2 + r_3 P_3 + \ldots + r_r P_r$$

mittelst der Koeffizienten $1_0, 1_1, 1_2, 1_3 \ldots 1_r$ zu bestimmen. Zu dem Ende bemerken wir auf Grund der in Nr. 1 aufgestellten Tafel der positiven und negativen Reste, dass für ein paares s keine der Kombinationen $P_1 P_2, P_1 P_3, \ldots P_1 P_r$ einen Nullrest haben kann, dass also $2_0 = 3^0 = \ldots r_0 = 0$ ist, dass aber in der ersten Kombination $P_1 P_1$ eine einzige Nullreihe erscheint, dass mithin $1_0 = 1$ ist.

Für ein unpaares s enthält $P_1 P_{m+1}$ diese eine Nullreihe, es ist also dann $(m + 1)_0 = 1$ und alle übrigen ersten Koeffizienten $1_0, 2_0, 3_0 \ldots m_0, (m + 2)_0, (m + 3)_0 \ldots r_0$ sind gleich null.

Da bei der Identifikation mit der Gleichung $x^p - 1 = 0$ für jeden Nullrest die Einheit zu setzen ist; so hat man allgemein $P_0 = s = \frac{p-1}{r}$.

Um hiernach die Tafel der Koeffizienten

$$\begin{array}{llllllll} \text{für } P_1\,P_1 & 1_1 & 1_2 & 1_3 & \ldots & 1_r \\ \text{„ } P_1\,P_2 & 2_1 & 2_2 & 2_3 & \ldots & 2_r \\ \text{„ } P_1\,P_3 & 3_1 & 3_2 & 3_3 & \ldots & 3_r \\ & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \text{„ } P_1\,P_r & r_1 & r_2 & r_3 & \ldots & r_r \end{array}$$

(von welcher wir die Koeffizienten 1_0, 2_0, 3_0 ... der Nullglieder ausgeschlossen haben) aufzustellen; so ergeben die Beziehungen (9) und (10), wenn man einmal α als konstant und β als variabel von 1 bis r ansieht, für den ersten Fall eines paaren s, bei geeigneter Bestimmung des β $\alpha_1 = 1_\alpha$ und $\alpha_\alpha = (r - \alpha + 2)_1$ oder auch $\alpha_1 = (r - \alpha + 2)_{r-\alpha+2}$ oder auch $(r - \alpha)_1 = (\alpha + 2)_{\alpha+2}$.

Die Beziehung (9) lehrt hiernach, dass eine Horizontalreihe und eine Vertikalreihe der Koeffiziententafel, deren Anfangsglied 1_α und α_1 gleich weit von dem ersten Reste 1_1 abstehen, dieselben Koeffizienten und in derselben Reihenfolge enthalten.

Die Beziehung (10) lehrt, dass eine Horizontalreihe vom ersten Gliede an dieselbe Koeffizientenfolge hat, wie eine andere Horizontalreihe, welche von oben um eine Stelle weiter, als diese von unten absteht, von dem in der Diagonale $1_1\ r_r$ liegenden Gliede an besitzt. Wenn in Fig. 6 im Quadrate I die Linien Horizontal- und Vertikalreihen der Koeffiziententafel darstellen; so hat die horizontale Reihe $a\,b\,c$, welche die Vertikalreihe $a\,b\,c$ in b kreuzt, die nämliche Koeffizientenfolge, wie die Letztere; auch hat jene Horizontalreihe von b über c nach a und b dieselbe Koeffizientenfolge wie die Horizontalreihe $b\,d$ von a aus, wenn die Strecke $A\,a$ eine Reihe mehr enthält, als die Strecke $B\,b$. In der Diagonalen $A\,C$ steht im Durchschnitte mit der Horizontalen $b\,c$ der Rest b und im Durchschnitte mit der Horizontalen $b\,d$ der Rest a; man kann also die Koeffizientenfolge $a\,b\,c$ in den drei mit a bezeichneten Punkten beginnen, indem man in der Richtung der Pfeile fortschreitet.

Für den zweiten Fall eines unpaaren s, welches ein paares $r = 2m$ voraussetzt, hat man die beiden Beziehungen

$$\alpha_1 = (m + 1)_{m+\alpha} \quad \text{und} \quad \alpha_\alpha = (r - \alpha + 2)_1$$

Wenn in dem Quadrate II der Fig. 6 die punktirte horizontale und vertikale Linie die m-te Reihe von der Ecke A bezeichnet; so beginnt die horizontale Reihe $a\,c$ in a mit denselben Koeffizienten, wie die vertikale Reihe $a\,b$, indem der Punkt a der letzteren Reihe in der $(m + 1)$-ten Horizontalreihe und in der $(m + \alpha)$-ten Vertikalreihe genommen wird. Ausserdem bleibt wie beim ersten Falle die horizontale Reihe $a\,b$ von a aus mit der horizontalen Reihe $a\,d$ von a aus identisch, sodass dieselbe Koeffizientenreihe von den drei Punkten a in der Richtung der Pfeile durchschnitten werden kann.

6) Die Aufstellung der Koeffiziententafel gestaltet sich zu einem ganz einfachen mechanischen Verfahren, wenn man beachtet, dass einunderselbe Koeffizient α_β nach den Formeln (9) und (10) an sechs Stellen erscheint

(wovon einige zusammenfallen). Im ersten Falle, für ein paares s, sind zwei dieser Werthe nach Gl. (9) durch die Formel $u_\beta = \beta_\alpha$, zwei andere nach Gl. (10) und (9) durch die Formel

$$(11) \qquad (r - \alpha + 2)_{\beta-\alpha+1} = (\beta - \alpha + 1)_{r-\alpha+2}$$

und wenn man α und β vertauscht nach Gl. (11) und (9) durch die Formel

$$(12) \qquad (r - \beta + 2)_{\alpha-\beta+1} = (\alpha - \beta + 1)_{r-\beta+2}$$

dargestellt. Von jedem dieser drei Stellenpaare liegt die eine Stelle links und die andere rechts von der Diagonalen $A\,C$ und zwar in gleichen normalen Abständen in einer zu der anderen Diagonalen $B\,D$ parallelen Linie. (In dem Koeffizienten 1_1 fallen alle sechs Stellen und in jedem anderen Koeffizienten 1_2, 1_3 ... 1_r der ersten Reihe fallen je zwei Stellen zusammen).

Zieht man in Fig. 7 durch den in der Diagonalen $A\,C$ liegenden Punkt a auch die vertikale Linie $a\,c$; so hat dieselbe die Koeffizientenfolge wie jede der drei Linien $a\,c$; es kömmt also jede Koeffizientenreihe viermal, zweimal in horizontaler und zweimal in vertikaler Linie vor. Die erste horizontale Reihe kreuzt die erste vertikale Reihe in dem Punkte f der Diagonalen $A\,C$, und die zweite horizontale kreuzt die zweite vertikale Reihe in dem Punkte a derselben Diagonalen, indem die Strecke $C\,a$ um eine Stelle kürzer ist, als die Strecke $A\,f$. Wenn der Koeffizient a in der horizontalen Reihe $a\,E$ gleich α_1 ist; so ist der ihm gleiche a in der vertikalen Reihe $a\,F$ gleich 1_α und der ihm ebenfalls gleiche a in der horizontalen Reihe $a\,G$, sowie in der vertikalen Reihe $a\,H$ gleich $(r - \alpha + 2)_{r-\alpha+2}$. Ein Koeffizient c, welcher einer solchen Reihe angehört, wenn es nicht der Anfangspunkt a selbst ist, erscheint also in den sechs aus der Fig. 7 ersichtlichen Stellen, welche in den Seiten eines Quadrates $b\,c\,d\,c$ so liegen, dass sie zwei Ecken desselben und ausserdem in jeder Seite eine Stelle einnehmen.

Wenn r ein Vielfaches von 3, also $= 3\,\mu$ ist; so findet sich für die Anzahl der unbekannten Koeffizienten der Werth

$$(13) \qquad \frac{1}{6}\,r\,(r + 3) + 1 = \frac{1}{6}\,(r^2 + 3\,r + 6)$$

und wenn r kein Vielfaches von 3, also entweder $= 3\,\mu + 1$ oder $= 3\,\mu + 2$ ist,

$$(14) \qquad \frac{1}{6}\,(r + 1)\,(r + 2) = \frac{1}{6}\,(r^2 + 3\,r + 2)$$

Diese Ausdrücke ergeben sich durch folgende Betrachtung. In der Koeffiziententafel bilden diese Unbekannten in ihrer ursprünglichen oder natürlichen Stellung zusammenhängende Strecken der obersten Horizontalreihen und füllen daselbst einen keilförmigen Ausschnitt, dessen oberste horizontale Linie die ganze erste Horizontalreihe umfasst, während die folgenden Linien sich immer um drei Stellen verkürzen (was nur für $r = 3\,\mu$ eine sogleich zu bezeichnende Ausnahme erleidet). Für $r = 3\,\mu + 1$ enthält hiernach die unterste Linie des fraglichen Keils einen und für $r = 3\,\mu + 2$ enthält sie zwei Stellen. Für $r = 3\,\mu$ tritt in die

unterste Linie, welche sich nach der vorstehenden Regel auf keine Stelle reduziren müsste, ein Koeffizient. Hiernach umfasst der Keil für $r = 3\mu + 1$ überhaupt $\frac{1}{3}(r + 2)$ für $r = 3\mu + 2$ überhaupt $\frac{1}{3}(r + 1)$ und für $r = 3\mu$ überhaupt $\frac{1}{3}(r + 3)$ horizontale Linien. Bezeichnen wir also den ersten Koeffizienten der letzten Reihe des Keiles mit x_y; so stellt sich dieser Keil für die drei Formen von r folgendermaassen dar.

1) $r = 3\mu + 1 \quad x = \frac{1}{3}(r + 2) \quad y = \frac{1}{3}(2r + 1)$

$1_1\ 1_2\ 1_3\ 1_4\ 1_5\ 1_6\ 1_7 \ldots\ldots\ldots\ldots 1_{r-3}\ 1_{r-2}\ 1_{r-1}\ 1_r$
$2_3\ 2_4\ 2_5\ 2_6\ 2_7 \ldots\ldots\ldots\ldots 2_{r-3}\ 2_{r-2}\ 2_{r-1}$
$3_5\ 3_6\ 3_7 \ldots\ldots\ldots\ldots 3_{r-3}\ 3_{r-2}$
$4_7 \ldots\ldots\ldots\ldots 4_{r-3}$
$\ldots\ldots\ldots$
$\ldots\ldots\ldots$
$(x-1)_{y-2}\ (x-1)_{y-1}\ (x-1)_y\ (x-1)_{y+1}$
x_y

2) $r = 3\mu + 2 \quad x = \frac{1}{3}(r + 1) \quad y = \frac{1}{3}(2r - 1)$

$1_1\ 1_2\ 1_3\ 1_4\ 1_5\ 1_6\ 1_7 \ldots\ldots\ldots\ldots 1_{r-3}\ 1_{r-2}\ 1_{r-1}\ 1_r$
$2_3\ 2_4\ 2_5\ 2_6\ 2_7 \ldots\ldots\ldots\ldots 2_{r-3}\ 2_{r-2}\ 2_{r-1}$
$3_5\ 3_6\ 3_7 \ldots\ldots\ldots\ldots 3_{r-3}\ 3_{r-2}$
$4_7 \ldots\ldots\ldots\ldots 4_{r-3}$
$\ldots\ldots\ldots$
$\ldots\ldots\ldots$
$x_y\ x_{y+1}$

3) $r = 3\mu \quad x = \frac{1}{3}(r + 3) \quad y = \frac{1}{3}(2r + 3)$

$1_1\ 1_2\ 1_3\ 1_4\ 1_5\ 1_6\ 1_7 \ldots\ldots\ldots\ldots 1_{r-3}\ 1_{r-2}\ 1_{r-1}\ 1_r$
$2_3\ 2_4\ 2_5\ 2_6\ 2_7 \ldots\ldots\ldots\ldots 2_{r-3}\ 2_{r-2}\ 2_{r-1}$
$3_5\ 3_6\ 3_7 \ldots\ldots\ldots\ldots 3_{r-3}\ 3_{r-2}$
$4_7 \ldots\ldots\ldots\ldots 4_{r-3}$
$\ldots\ldots\ldots$
$\ldots\ldots\ldots$
$(x-1)_{y-2}\ (x-1)_{y-1}\ (x-1)_y$
x_y

Die oberste horizontale, die erste vertikale und die diagonale Reihe enthalten sämmtliche Koeffizienten der ersten Reihe in derselben Reihenfolge, und man übersieht leicht den Mechanismus, nach welchem die Tafel

aufzustellen ist, indem man immer auf die zuletzt gebildete Horizontalreihe die dieselbe in der Diagonalen kreuzende Vertikalreihe und die mit ihr korrespondirende Horizontalreihe, sowie die diese in der Diagonalen kreuzende Vertikalreihe herstellt.

Für $r = 2, 3, 4, 5, 8$ sind diese Tafeln

für $r = 2$

1_1	1_2
1_2	1_2

für $r = 3$

1_1	1_2	1_3
1_2	1_3	2_3
1_3	2_3	1_2

für $r = 4$

1_1	1_2	1_3	1_4
1_2	1_4	2_3	2_3
1_3	2_3	1_3	2_3
1_4	2_3	2_3	1_2

für $r = 5$

1_1	1_2	1_3	1_4	1_5
1_2	1_5	2_3	2_4	2_3
1_3	2_3	1_4	2_4	2_4
1_4	2_4	2_4	1_3	2_3
1_5	2_3	2_4	2_3	1_2

für $r = 8$

1_1	1_2	1_3	1_4	1_5	1_6	1_7	1_8
1_2	1_8	2_3	2_4	2_5	2_6	2_7	2_3
1_3	2_3	1_7	2_7	3_5	3_6	3_5	2_4
1_4	3_4	2_7	1_6	2_6	3_6	3_6	2_5
1_5	2_3	3_5	2_6	1_5	2_5	3_5	2_6
1_6	2_6	3_6	3_6	2_5	1_4	2_4	2_7
1_7	2_7	3_5	3_6	3_5	2_4	1_3	2_3
1_8	2_3	2_4	2_5	2_6	2_7	2_3	1_2

7) Wir haben jetzt den zweiten Fall, eines unpaaren s, welches ein paares $r = 2m$ voraussetzt, zu erörtern. Auch hier erscheint jeder Koeffizient (ausser gewissen einzelnen) an sechs Stellen, welche unter Berücksichtigung der Relation $u_\beta = (u \pm r)_{\beta \pm r}$ folgenden Werthen entsprechen.

$$u_\beta = (\beta + m)_{\alpha+m}$$

$$(15) \qquad (r - u + 2)_{\beta-\alpha+1} = (\beta - u + 1 + m)_{r-\alpha+2+m}$$

$$(16) \qquad (r - \beta + m + 2)_{\alpha-\beta+1} = (\alpha - \beta + 1 + m)_{r-\beta+2}$$

Diese Werthe liegen auch hier in zwei horizontalen und zwei vertikalen, überhaupt in vier Reihen, welche dieselbe Koeffizientenfolge haben. Diese vier Reihen sind in Fig. 8 dargestellt, indem die mit a bezeichneten vier Stellen denselben Koeffizienten aufnehmen. Wenn der Koeffizient a in der horizontalen Reihe $a\ E$ gleich u_1 ist; so ist der ihm gleiche a in der vertikalen Reihe $a\ F$ gleich $(m + 1)_{m+\alpha}$, der ihm gleiche a in der horizontalen Reihe $a\ G$ gleich $(r - u + 2)_{r-\alpha+2}$ und der ihm ebenfalls gleiche a in der vertikalen Reihe $a\ H$ gleich $(m - u + 2)_{m-\alpha+2}$. Die Koeffizientenfolge der ersten Horizontalreihe erscheint in derjenigen Vertikalreihe wieder, welche durch die Stelle $m + 1$ geht, wobei der erste Koeffizient 1_1 mit $(m + 1)_{m+1}$ übereinstimmt.

Die Anzahl der unbekannten Koeffizienten wird auch jetzt durch die Formel (13) oder (14) ausgedrückt, jenachdem r die Form 3μ oder eine der beiden Formen $2\mu + 1$, $2\mu + 2$ hat; sie nehmen aber in der Tafel eine ganz andere Stellung ein, als bei einem paaren s: sie füllen nämlich darin die linke und die rechte obere Ecke bei A und D und zwar dergestalt aus, dass in jeder tieferen Horizontallinie drei Stellen weniger ausgefüllt sind, als in der vorhergehenden (mit der obigen Ausnahme der letzten Reihe für $r = 3\mu$). Hiernach umfassen die beiden Eckkeile mit den unbekannten Koeffizienten auch resp. $\frac{1}{3}(r + 2)$, $\frac{1}{3}(r + 1)$, $\frac{1}{3}(r + 3)$ horizontale Reihen, jenachdem $r = 3\mu + 1$, $3\mu + 2$, 3μ ist. Für $r = 4, 6, 8, 10, 12$ enthalten die fraglichen Eckkeile folgende Koeffizienten

$r = 4$

1_1	1_2	1_3	1_4	
2_1				

$r = 6$

1_1	1_2	1_3	1_4	1_5	1_6
2_1	2_2	2_3			
	3_2				

$r = 8$

1_1	1_2	1_3	1_4	1_5	1_6	1_7	1_8
2_1	2_2	2_3	2_4				2_8
3_1	3_2						

$r = 10$

1_1	1_2	1_3	1_4	1_5	1_6	1_7	1_8	1_9	1_{10}
2_1	2_2	2_3	2_4	2_5				2_9	2_{10}
3_1	3_2	3_3	3_4						
	4_2								

$r = 12$

1_1	1_2	1_3	1_4	1_5	1_6	1_7	1_8	1_9	1_{10}	1_{11}	1_{12}
2_1	2_2	2_3	2_4	2_5	2_6				2_{10}	2_{11}	2_{12}
3_1	3_2	3_3	3_4	3_5							3_{12}
4_1	4_2	4_3									
		5_3									

Die vollständigen Koeffiziententafeln für $r = 2, 4, 8$ sind

für $r = 2$

1_1	1_2
1_1	1_1

für $r = 4$

1_1	1_2	1_3	1_4
2_1	2_1	1_4	1_2
1_1	2_1	1_1	2_1
2_1	1_4	1_2	2_1

für $r = 8$

1_1	1_2	1_3	1_4	1_5	1_6	1_7	1_8
2_1	2_2	2_3	2_4	1_6	1_4	2_4	2_8
3_1	3_2	3_1	2_8	1_7	2_4	1_3	2_3
2_2	3_2	3_2	2_1	1_8	2_8	2_3	1_2
1_1	2_1	3_1	2_2	1_1	2_1	3_1	2_2
2_1	1_8	2_8	2_3	1_2	2_2	3_2	3_2
3_1	2_8	1_7	2_4	1_3	2_3	3_1	3_2
2_2	2_3	2_4	1_6	1_4	2_4	2_8	2_1

Für alle Rechnungen, bei welchen es nur auf die in jeder der Kombinationen $P_1 P_1$, $P_1 P_2$, $P_1 P_3$ ... enthaltenen Koeffizienten, nicht auf deren Reihenfolge ankömmt, ist es wichtig, dass sich für einen beliebigen Werth von $r = 2m$ aus der Koeffiziententafel für ein paares s die Koeffiziententafel für ein unpaares s, oder umgekehrt, aus dieser jene ergiebt, wenn man die beiden Koeffizienten 1_0 und m_0, ausserdem aber je zwei Koeffizienten k_x und k_{x+m} oder deren äquivalente Werthe $k_{x \pm r}$ und $k_{x+m \pm r}$ miteinander vertauscht. So geht z. B. für $r = 8$ die Koeffiziententafel für ein paares s in die für ein unpaares über, wenn man resp.

$$1_0\ 1_1\ 1_2\ 1_3\ 1_4\ 1_5\ 1_6\ 1_7\ 1_8\ 2_3\ 2_4\ 2_5\ 2_6\ 2_7\ 3_5\ 3_6$$

durch $$4_0\ 1_5\ 1_6\ 1_7\ 1_8\ 1_1\ 1_2\ 1_3\ 1_4\ 2_7\ 2_8\ 2_1\ 2_2\ 2_3\ 3_1\ 3_2$$

ersetzt (indem für ein paares s $2_8 = 2_3$ und für ein unpaares s $2_7 = 2_4$ ist).

8) Wenn alle Koeffizienten der vorstehenden Tafel bekannt sind, ergeben die in Nr. 5 aufgestellten Formeln unter Zuziehung der bekannten Koeffizienten 1_0, 2_0, 3_0 ... der Nullglieder die Werthe der zweidimensionalen Kombinationen $P_1 P_1$, $P_1 P_2$, $P_1 P_3$ ..., deren erster Faktor P_1 ist. Durch einfache Verschiebung der Koeffizienten (mit Ausnahme des Koeffizienten des Nullgliedes) folgen hieraus die Werthe aller möglichen zweidimensionalen Kombinationen, wie

$$P_2 P_2,\ P_3 P_3 \ldots,\ P_2 P_3,\ P_3 P_4 \ldots,\ P_2 P_4,\ P_3 P_5 \ldots \text{ etc.}$$

Aus den zweidimensionalen Kombinationen ergeben sich alle dreidimensionalen. Denn wenn

$$P_\alpha P_\beta = \varrho_0 P_0 + \varrho_1 P_1 + \varrho_2 P_2 + \ldots$$

bekannt ist; so lässt sich daraus

$$P_\alpha P_\beta P_\gamma = \varrho_0 P_0 P_\gamma + \varrho_1 P_1 P_\gamma + \varrho_2 P_2 P_\gamma + \ldots$$

herstellen, indem man für die zweidimensionalen Kombinationen $P_1 P_\gamma$, $P_2 P_\gamma$ ... ihre durch P_0, P_1, P_2 ... ausgedrückten Werthe substituirt und beachtet, dass $P_0 = s$ ist.

Aus den dreidimensionalen ergeben sich auf dieselbe Weise die vierdimensionalen und alle höher dimensionirten Kombinationen als Summen eindimensionaler Glieder mit Koeffizienten, welche sämmtlich durch die obigen Koeffizienten bestimmt sind.

9) Sobald eine n-dimensionale Kombination $P_\alpha P_\beta P_\gamma \ldots$ in der linearen Form

(17) $$P_\alpha P_\beta P_\gamma = \varphi_0 P_0 + \varphi_1 P_1 + \varphi_2 P_2 + \ldots + \varphi_r P_r$$

bekannt ist, hat man für die primitive zyklische Reihe $F(P_\alpha P_\beta P_\gamma \ldots)$, wenn sie aus r Gliedern besteht,

$$F(P_\alpha P_\beta P_\gamma \ldots) = r\,\varphi_0 P_0 + (\varphi_1 + \varphi_2 + \ldots + \varphi_r)(P_1 + P_2 + \ldots + P_r)$$

oder da $P_1 + P_2 + \ldots + P_r = Y$ ist, indem man $\varphi_1 + \varphi_2 + \ldots + \varphi_r = \eta$ setzt,

$$(18)\quad F(P_\alpha P_\beta P_\gamma \ldots) = r\,\varphi_0 P_0 + \eta Y$$

Wegen der gegebenen Gleichung ist stets

$$(19)\qquad s^n = \varphi_0 s + \eta s \qquad \text{oder} \qquad \eta = s^{n-1} - \varphi_0$$

mithin, wenn man $P_0 = s$ und $Y = -1$ setzt,

$$(20)\quad F(P_\alpha P_\beta P_\gamma \ldots) = \varphi_0 p - s^{n-1}$$

Angenommen nun, die n-dimensionale zyklische Reihe $F(P_\alpha P_\beta P_\gamma \ldots)$ bestehe aus r' Gliedern, sodass also die erste Kombination $P_\alpha P_\beta P_\gamma \ldots$ nach r' Verschiebungen wiederkehrt; so wird r' ein Faktor von r und es wird

$$\varphi_1 = \varphi_{r'+1} = \varphi_{2r'+1} = \text{etc.}$$
$$\varphi_2 = \varphi_{r'+2} = \varphi_{2r'+2} = \text{etc.}$$
$$\varphi_3 = \varphi_{r'+3} = \varphi_{2r'+3} = \text{etc.}$$

überhaupt $\varphi_x = \varphi_{mr'+x}$ und

$$(21)\quad \varphi_1 + \varphi_2 + \ldots + \varphi_{r'} = \varphi_{r'+1} + \varphi_{r'+2} + \ldots + \varphi_{2r'}$$
$$= \varphi_{2r'+1} + \varphi_{2r'+2} + \ldots + \varphi_{3r'}$$
$$\text{etc.} \qquad = \frac{r'}{r}(\varphi_1 + \varphi_2 + \ldots + \varphi_r) = \frac{r'}{r}\eta$$

sein. Diese letzteren Summen stellen zugleich die Koeffizienten der Grössen $P_1, P_2, P_3 \ldots$ der r'-gliedrigen symmetrischen Funktion $F(P_\alpha P_\beta P_\gamma \ldots)$ dar, während der Koeffizient von P_0 gleich $r'\varphi_0$ ist; man hat daher

$$F(P_\alpha P_\beta P_\gamma \ldots) = r'\varphi_0 P_0 + \frac{r'}{r}\eta Y$$

und wegen $P_0 = s$, $Y = -1$, $\eta = s^{n-1} - \varphi_0$

$$(22)\quad F(P_\alpha P_\beta P_\gamma \ldots) = \frac{r'}{r}(\varphi_0 p - s^{n-1})$$

Dieser beachtenswerthe Ausdruck liefert für die r-dimensionale symmetrische Funktion $P_1 P_2 \ldots P_r$, welche aus einem einzigen Gliede besteht, den Werth

$$(23)\qquad P_1 P_2 \ldots P_r = \frac{1}{r}(\varphi_0 p - s^{r-1})$$

Besteht die n-dimensionale Funktion F aus mehreren primitiven symmetrischen Reihen von resp. $r', r'', r''' \ldots$ Gliedern; so ergiebt die Formel (22), indem man $r' + r'' + r''' + \ldots = r_1$ setzt,

$$(24)\qquad F_n = (r'\varphi_0' + r''\varphi_0'' + r'''\varphi_0''' + \ldots)\frac{p}{r} - \frac{r'}{r}s^{n-1}$$

Wenn r eine Primzahl ist, haben nach §. 4 alle primitiven Reihen (mit Ausnahme der eingliedrigen r-dimensionalen Funktion) r Glieder und ihre Anzahl ist $= \frac{1}{r}\,{}^{r}B_{n}$, worin ${}^{r}B_{n}$ den n-ten Binomialkoeffizienten der r-ten Potenz bezeichnet. Demnach ist für diesen Fall die n-dimensionale Funktion

$$(25)\qquad F_{n} = (\varphi_{0}' + \varphi_{0}'' + \varphi_{0}''' + \ldots)\,p - {}^{r}B_{n}\,\frac{s^{n-1}}{r}$$

$$= (\varphi_{0}' + \varphi_{0}'' + \varphi_{0}''' + \ldots)\,p - {}^{r}B_{n}\,\frac{(p-1)^{n-1}}{r^{n}}$$

während F_{r} immer nach Gl. (23) zu bestimmen ist.

10) Wenn irgend eine Funktion f der Grössen P bei der zyklischen Verschiebung ungeändert bleibt; so müssen in ihrem linearen Ausdrucke

$$f\,(P_{\alpha}\,P_{\beta}\,P_{\gamma}\ldots) = \psi_{0}\,P_{0} + \psi_{1}\,P_{1} + \psi_{2}\,P_{2} + \ldots + \psi_{r}\,P_{r}$$

die r Koeffizienten $\psi_{1}, \psi_{2} \ldots \psi_{r}$ einander gleich und daher jene Funktion

$$f = \psi_{0}\,P_{0} + \psi_{1}\,Y = \psi_{0}\,s - \psi_{1}$$

sein. Denn die Verschiebung um eine Stelle ergiebt den Ausdruck $\psi_{0}\,P_{0} + \psi_{r}\,P_{1} + \psi_{1}\,P_{2} + \ldots + \psi_{r-1}\,P_{r}$, welcher mit dem vorstehenden nur übereinstimmen kann, wenn $\psi_{1} = \psi_{2} = \ldots = \psi_{r}$ ist.

Ist die unveränderliche Funktion n-dimensional und besteht sie aus r_{1} Gliedern; so ist offenbar

$$r_{1}\,s^{n} = \psi_{0}\,s + \psi_{1}\,r\,s, \quad \text{also} \quad \psi_{1} = \frac{1}{r}\,(r_{1}\,s^{n-1} - \psi_{0})$$

Für die aus einem einzigen Gliede bestehende r-dimensionale Funktion $P_{1}\,P_{2}\ldots P_{r}$ ist $\psi_{1} = \frac{1}{r}\,(s^{r-1} - \psi_{0})$ und

$$P_{1}\,P_{2}\ldots P_{r} = \psi_{0}\,P_{0} - \psi_{1} = \frac{1}{r}\,(\psi_{0}\,p - s^{r-1})$$

wie nach Gl. (23).

11) Nach Vorstehenden kömmt es also wesentlich auf die Bestimmung der Koeffizienten der obigen Tafel und zwar der vorhin bezeichneten an. Hierzu dienen zunächst für jeden beliebigen Werth von s, gleichviel, ob $r = 2m$, oder $= 2m + 1$ ist, die Ausdrücke für die $m + 1$ Kombinationen $P_{1}\,P_{1}$, $P_{1}\,P_{2}$, $\ldots$ $P_{1}\,P_{m+1}$. Da jede solche Kombination s^{2} Glieder, ein einfaches P aber s Glieder hat; so ergeben sich die $m + 1$ Beziehungen in Gestalt der Gleichungen ersten Grades

$$(26)\qquad \begin{cases} 1_{0} + 1_{1} + 1_{2} + \ldots + 1_{r} = s \\ 2_{0} + 2_{1} + 2_{2} + \ldots + 2_{r} = s \\ 3_{0} + 3_{1} + 3_{2} + \ldots + 3_{r} = s \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ (m+1)_{0} + (m+1)_{1} + (m+1)_{2} + \ldots + (m+1)_{r} = s \end{cases}$$

Zur Bestimmung der in Nr. 6 erwähnten Anzahl von Unbekannten

fehlen also noch, jenachdem r die Form $6v$, $6v+1$, $6v+2$, $6v+3$, $6v+4$, $6v+5$ hat, folgende Anzahl von Gleichungen

für $r = 6v$	fehlen	$\frac{1}{6} r^2$	oder $6v^2$	Gleichungen
„ $r = 6v+1$	„	$\frac{1}{6}(r^2-1)$	„ $6v^2+2v$	„
„ $r = 6v+2$	„	$\frac{1}{6}(r^2-4)$	„ $6v^2+4v$	„
„ $r = 6v+3$	„	$\frac{1}{6}(r^2+3)$	„ $6v^2+6v+2$	„
„ $r = 6v+4$	„	$\frac{1}{6}(r^2-4)$	„ $6v^2+8v+2$	„
„ $r = 6v+5$	„	$\frac{1}{6}(r^2-1)$	„ $6v^2+10v+4$	„

Für $r = 6v+3$ kann die fehlende Anzahl auch $= \frac{1}{6}(r^2-9)+2$ gesetzt werden.

12) Die Kombinationen $P_1 P_n$, worin $n > m+1$ ist, liefern, da sie zyklische Verschiebungen der früheren sind, keine neuen Beziehungen. Aber auch die Kombinationen von mehr als zwei Dimensionen liefern nicht sämmtlich neue Beziehungen zwischen den fraglichen Koeffizienten durch Gleichsetzung der Gliederzahl auf beiden Seiten. Beispielsweise ergiebt sich aus

$$P_1 P_2 = 2_0 P_0 + 2_1 P_1 + 2_2 P_2 + \ldots + 2_r P_r$$

$$\begin{aligned} P_1 P_1 P_2 &= 2_0 P_0 P_1 + 2_1 P_1 P_1 + 2_2 P_1 P_2 + \ldots + 2_r P_1 P_r \\ &= 2_0 P_0 P_1 \\ &\quad + 2_1 1_0 P_0 + 2_1 1_1 P_1 + 2_1 1_2 P_2 + \ldots + 2_1 1_r P_r \\ &\quad + 2_2 2_0 P_0 + 2_2 2_1 P_1 + 2_2 2_2 P_2 + \ldots + 2_2 2_r P_r \\ &\quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\quad + 2_r r_0 P_0 + 2_r r_1 P_1 + 2_r r_2 P_2 + \ldots + 2_r r_r P_r \end{aligned}$$

Da $P_1 P_1 P_2$ überhaupt s^3, jedes P aber s Glieder hat; so folgt

$$\begin{aligned} s^2 &= 2_0 P_0 + 2_1 (1_0 + 1_1 + \ldots + 1_r) + 2_2 (2_0 + 2_1 + \ldots + 2_r) \\ &\quad + \ldots + 2_r (r_0 + r_1 + \ldots + r_r) \end{aligned}$$

und wegen der Gleichungen (26) $s^2 = 2_0 P_0 + (s - 2_0) s$, eine Formel, welche wegen $P_0 = s$ nur eine Identität darstellt.

13) Auch die Darstellung höherer Potenzen von P_1 als Summe eindimensionaler Glieder in der Form

$$(P_1)^r = 1_0 P_0 + 1_2 P_1 + 1_2 P_2 + \ldots + 1_r P_r$$

um aus den Koeffizienten 1_0, 1_1, 1_2 ... (welche jetzt andere Werthe als vorhin haben), die Werthe der gleichdimensionalen Kombinationen

$(P_1)^{v-1}\ P_2$, $(P_1^{v-1})\ P_3$, $(P_1^{v-2})\ P_2\ P_3$, etc. herzustellen, verhilft nicht zu wesentlich neuen Relationen. Übrigens sind zu dieser Darstellung folgende Beziehungen wichtig.

Wenn die Gleichung

$$1 + 1 + \ldots + a^x + a^y + a^z = a^u$$

besteht; so ergiebt eine Transposition von a^z und a^u, da $p - 1 = rs$ ist,

$$1 + 1 + \ldots + a^x + a^y + a^{u+\frac{1}{2}rs} = a^{z+\frac{1}{2}rs}$$

oder für ein paares s

$$a^0 + a^0 + \ldots + a^x + a^y + a^u = a^z$$

und für ein unpaares s, welches ein paares $r = 2m$ voraussetzt,

$$a^0 + a^0 + \ldots + a^x + a^y + a^{u+m} = a^{z+m}$$

So oft also die Kombination $(P_1)^v\ P_x\ P_y\ P_z$ einen Rest der Reihe P_u liefert, ebenso oft liefert im ersten Falle die Kombination $(P_1)^v\ P_x\ P_y\ P_u$ einen Rest der Reihe P_z und im zweiten Falle die Kombination $(P_1)^v\ P_x\ P_y\ P_{u+m}$ einen Rest der Reihe P_{z+m}.

Multiplizirt man die gegebene Gleichung mit a^{r-x}; so kömmt

$$a^{r-x} + a^{r-x} + \ldots + a^r + a^{r+y-x} + a^{r+z-x} = a^{r+u-x}$$

So oft also die Kombination $(P_1)^v\ P_x\ P_y\ P_z$ einen Rest der Reihe P_u liefert, ebenso oft liefert in beiden Fällen die Kombination $(P_{r-x+2})^v\ P_1\ P_{y-x+1}\ P_{z-x+1}$ einen Rest der Reihe P_{u-x+1}.

In diesen Formeln kann auf der linken Seite die Anzahl v der gleichen und die Anzahl der ungleichen Faktoren eine beliebige sein; es können sich unter den letzteren auch wieder beliebig viel gleiche befinden.

Im Allgemeinen führt der Ausgang von den in Nr. 5 aufgestellten Werthen der zweidimensionalen Funktionen am bequemsten zu den gesuchten Beziehungen.

14) Weder die zyklische Verschiebung einer Kombination, noch die Erhöhung derselben durch Multiplikation mit einer Grösse P_n unter Substitution der linearen Werthe für $P_1\ P_n$, $P_2\ P_n$, $P_3\ P_n$ ... kann neue oder selbstständige Beziehungen zwischen den Koeffizienten dadurch liefern, dass man die Gliederzahl auf beiden Seiten der erhaltenen Gleichung einander gleich setzt. Demnach kann auch keine symmetrische Funktion, deren Glieder eine zyklische Reihe bilden, also durch Verschiebung entstehen, neue Beziehungen erzeugen. Nur, wenn aus der vorstehenden Multiplikation mit den Grössen P_n unmittelbar, oder doch ohne zyklische Verschiebung und Addition der verschobenen Glieder eine Funktion hervorginge, welche symmetrisch wäre, also durch Erhöhung aller Zeiger keine Veränderung erlitte, würden zu den $(m + 1)$ Beziehungen aus Nr. 11 noch diejenigen hinzutreten, welche sich aus der Gleichsetzung der Koeffizienten von P_1, P_2, P_3 ... in dieser Funktion ergeben. Unter den einfachen Kombinationen der Grössen P_1, P_2, ... P_r giebt es nur eine einzige, welche zugleich eine symmetrische Funktion ist, nämlich die r-dimensionale Kombination $P_1\ P_2 \ldots P_r$. Diese liefert durch Gleich-

setzung ihrer Koeffizienten nach Nr. 9 oder 10 überhaupt $r - 1$ Relationen, unter welchen sich neue befinden. Diese letzteren Beziehungen sind Gleichungen, deren Glieder Produkte von $r - 1$ der unbekannten Koeffizienten enthalten. Zu den $m + 1$ Beziehungen ersten Grades gesellen sich also Beziehungen vom $(r - 1)$-ten Grade. In keinem Falle (mit Ausnahme des Falles $r = 2$) werden sich so viel selbstständige Beziehungen ergeben, als unbekannte Koeffizienten vorhanden sind, da sich hierunter jedenfalls Gleichungen von einem höheren, als dem ersten Grade befinden, deren Auflösung nicht lauter ganze Zahlen für die gesuchten Koeffizienten ergeben könnte, wie es unbedingt erforderlich ist. Vielmehr muss die Anzahl der Relationen nothwendig kleiner bleiben, als die der zu bestimmenden Koeffizienten, sodass schliesslich eine gewisse Anzahl unbestimmter Gleichungen höherer Grade, welche eine Auflösung in ganzen Zahlen möglich machen, zur Erscheinung kommen.

Da jede symmetrische Funktion ein Inbegriff von zyklischen Reihen ist, jede solche Reihe aber als ein Resultat zyklischer Verschiebungen keine andere Relation der Koeffizienten involvirt, als ein einzelnes Glied der Reihe; so kann auch ein Inbegriff solcher Reihen nicht mehr neue Relationen liefern, als seine einzelnen Glieder. Zum Aufsuchen neuer Beziehungen eignet sich daher vornehmlich die r-dimensionale Kombination $P_1\ P_2 \ldots P_r$, welche zugleich eine symmetrische Funktion ist. Ist für irgend einen Werth von n die n-dimensionale Kombination $P_1\ P_2 \ldots P_n$ in der linearen Form

$$P_1\ P_2 \ldots P_n = \pi_0\ P_0 + \pi_1\ P_1 + \pi_2\ P_2 + \ldots + \pi_r\ P_r$$

gefunden; so ergeben sich die Koeffizienten ϱ_0, ϱ_1, $\varrho_2 \ldots \varrho_r$ der nächstfolgenden, $(n + 1)$-dimensionalen Kombination.

$$27)\quad P_1\ P_2 \ldots P_{n+1} = \varrho_0\ P_0 + \varrho_1\ P_1 + \varrho_2\ P_2 + \ldots + \varrho_r\ P_r$$

wenn man die vorstehende Gleichung mit P_n multiplizirt und für die alsdann erscheinenden zweidimensionalen Kombinationen $P_1\ P_n$, $P_2\ P_n$, $\ldots\ P_n\ P_r$ die linearen Ausdrücke aus Nr. 5 (resp. die durch Verschiebung daraus entstehenden) substituirt.

Für $n = r$ liefert die r-dimensionale Funktion $P_1\ P_2 \ldots P_r$ nach Nr. 10 durch Gleichsetzung der r Koeffizienten ϱ_1, ϱ_2, $\varrho_3 \ldots \varrho_r$ überhaupt $r - 1$ Gleichungen. Unter diesen Gleichungen können sich Identitäten befinden, wodurch sich die Zahl der selbstständigen Gleichungen vermindert. Sind keine Identitäten vorhanden; so hat man in diesen $r - 1$ Gleichungen und in den $m + 1$ Gleichungen (20) die grösstmögliche Anzahl von $m + r$ selbstständigen Gleichungen zwischen den unbekannten Koeffizienten: wir werden übrigens sehen, dass sich statt der Gleichungen vom Grade $r - 1$ auch Gleichungen niedrigeren Grades aufstellen lassen.

Nach diesen Rekursionsformeln (worin n nicht grösser, als $r - 1$ werden und jede Zahl x, welche $> r$ wird, gleich $x - r$ zu setzen ist), können die Koeffizienten der r-dimensionalen Kombination für $r = 2, 3, 4 \ldots$ leicht niedergeschrieben werden.

15) Die $m + 1$ Gleichungen ersten Grades aus Nr. 11 sind nach Maassgabe der für $r = 2, 3, 4$ sich ergebenden Koeffizententafeln

	I., für ein paares s	II., für ein unpaares s
für $r = 2$	$1_1 + 1_2 = s - 1$	$1_1 + 1_2 = s$
	$2 \cdot 1_2 = s$	$2 \cdot 1_1 = s - 1$
für $r = 3$	$1_1 + 1_2 + 1_3 = s - 1$	
	$1_2 + 1_3 + 2_3 = s$	
für $r = 4$	$1_1 + 1_2 + 1_3 + 1_4 = s - 1$	$1_1 + 1_2 + 1_3 + 1_4 = s$
	$1_2 + 1_4 + 2 \cdot 2_3 = s$	$1_2 + 1_4 + 2 \cdot 2_1 = s$
	$2(1_3 + 2_3) = s$	$2(1_1 + 2_1) = s - 1$
für $r = 5$	$1_1 + 1_2 + 1_3 + 1_4 + 1_5 = s - 1$	
	$1_2 + 1_5 + 2 \cdot 2_3 + 2_4 = s$	
	$1_3 + 1_4 + 2_3 + 2 \cdot 2_4 = s$	

16) Für $r = 2$ reichen die $m + 1$ Beziehungen aus, um alle Koeffizienten zu bestimmen: die zweidimensionale Funktion $P_1 P_2 = 2_0 P_0 + 2_1 P_1 + 2_2 P_2$ liefert auch keine weitere Beziehung zwischen den Koeffizienten. Wenn s paar $= 2\mu$, also die Primzahl $p = 4\mu + 1$ ist, ergiebt sich $1_1 = \frac{1}{4}(p - 5) = \mu - 1$ und $1_2 = \frac{1}{4}(p-1) = \mu$. Wenn s unpaar $= 2\mu + 1$, also $p = 4\mu + 3$ ist, ergiebt sich $1_1 = \frac{1}{4}(p - 3) = \mu$ und $1_2 = \frac{1}{4}(p + 1) = \mu + 1$.

17) Für $r = 3$ hat man zur Bestimmung der vier Unbekannten $1_1, 1_2, 1_3, 2_3$ nur zwei Gleichungen, es fehlen also noch deren zwei. Die dreidimensionale Funktion $P_1 P_2 P_3$ liefert nur eine einzige Relation: denn nach der Koeffiziententafel für $r = 3$ erweisen sich die beiden Werthe für ϱ_1 und ϱ_2 identisch $= 1_2 1_3 + 1_3 2_3 + 2_3 1_2$ und die Beziehungen $\varrho_1 = \varrho_2 = \varrho_3 = \frac{1}{3}(s^2 - 2_3)$ liefern nur die eine Gleichung

$$(28) \qquad 1_2 1_3 + 1_3 2_3 + 2_3 1_2 = 1_2 1_2 + 1_3 1_3 + 2_3 1_1$$

Eliminirt man aus den ersten beiden Gleichungen die Grösse s; so kömmt

$$(29) \qquad 2_3 = 1 + 1_1$$

und hierdurch wird die vorhergehende Gleichung, wenn man 2_3 eliminirt,

$$(30) \quad (1_1)^2 + (1_2)^2 + (1_3)^2 - (1_1 1_2 + 1_2 1_3 + 1_3 1_1) + 1_1 - 1_2 - 1_3 = 0$$

oder wenn man 1_1 eliminirt,

$$(31) \quad (1_2)^2 + (1_3)^2 + (2_3)^2 - (1_2 1_3 + 1_2 2_3 + 1_3 2_3) - 2_3 = 0$$

Die Gleichung (30) oder (31) ist eine quadratische mit drei Unbekannten, welche von s oder der Primzahl p ganz unabhängig ist. Sie liefert eine Reihe von Auflösungen in ganzen Zahlen, von welchen

diejenigen auszuwählen sind, die zugleich eine der beiden Gleichungen ersten Grades zwischen diesen Unbekannten und s erfüllen (da die zweite dieser beiden Gleichungen bereits durch die aus der Elimination von s hervorgegangene Gleichung (29) erfüllt wird).

Eliminirt man zwischen den beiden Gleichungen ersten Grades die Grösse s nicht; so kann man zwei Unbekannte mittelst s ausdrücken: man hat nämlich

$$(32) \qquad \begin{cases} 2_3 = 1 + 1_1 \\ 1_3 = s - 1 - 1_1 - 1_2 \end{cases}$$

Hierdurch verwandelt sich die Gl. (28) in eine quadratische Gleichung mit zwei Unbekannten.

$$(33) \quad 3\,1_1^2 + 3\,1_2^2 + 3\,1_1\,1_2 + 2\,1_1 - 3\,(s-1)\,(1_1 + 1_2) = -\,(s-1)\,(s-2)$$

Die Rücksicht auf die beiden Gleichungen ersten Grades bedingt keine Auswahl zwischen den Auflösungen der letzten Gleichung, da jene Gleichungen durch die anderen beiden Unbekannten 1_3 und 2_3 nach den Beziehungen (32) stets erfüllt werden.

Jede Auflösung der Gl. (33) entspricht also den Bedingungen der Aufgabe. Man ersieht hieraus, dass die Aufgabe überhaupt eine unbestimmte ist oder dass die Koeffizienten der Reihen für $P_1\ P_2$, $P_1\ P_3$, ... $P_1\ P_r$, mithin diese Reihen selbst und demzufolge auch die symmetrischen Funktionen der Grössen P_1, P_2, ... P_r, folglich diese Grössen selbst unbestimmte Werthe haben oder, mit anderen Worten, dass die Reste der Grundtafel verschiedene Perioden bilden können. Hieraus ist ersichtlich, dass diese Perioden von der primitiven Wurzel a, durch welche sie gebildet sind, mit abhängen. Nur für $r = 2$ haben die fraglichen Koeffizienten bestimmte Werthe (vgl. §. 1 Nr. 17).

Da es für jede Primzahl p nur eine bestimmte Anzahl von primitiven Wurzeln giebt; so kann die Anzahl der verschiedenen Auflösungen der Gl. (33) offenbar keine unendliche, sondern nur eine endliche sein, welche mit der Anzahl der primitiven Wurzeln a in einer gesetzlichen Beziehung stehen wird (wogegen die Anzahl der Auflösungen der Gl. (30) oder (31) möglicherweise eine unendliche sein könnte).

Die Gl. (29) und auch (31) ist für die beiden Grössen 1_2 und 1_3 symmetrisch gebildet, lehrt also, dass diese beiden Unbekannten stets ihre Werthe vertauschen können.

Wir heben hervor, dass die Gl. (33) das Problem vollständig lös't, indem sie alle für 1_1 und 1_2 und alsdann vermittelst der Beziehungen (32) alle für 1_3 und 2_3 möglichen oder zulässigen Werthe und nur diese unzweideutig liefert. Die aus der Kummerschen Theorie von Bachmann in der Lehre von der Kreistheilung auf S. 212 abgeleitete Formel dagegen lös't die Aufgabe nicht vollständig, indem die dort gefundenen Werthe der Koeffizienten von zwei Grössen (α und β) abhängig bleiben, welche nur ihrer Qualität, nicht aber ihrem Zeichen nach bestimmt sind, welche also jene Koeffizienten unbestimmt lassen, ja noch nicht einmal die Ganzzahligkeit derselben verbürgen.

Bachmann gelangt zu der aus der Formel (30) mit Hülfe der vorhergehenden Beziehungen leicht nachweisbaren Gleichung

$$(34) \qquad (6\,2_3 - 3\,1_2 - 3\,1_3 - 2)^2 + 27\,(1_2 - 1_3)^2 = 4p$$

welche die Form $A^2 + 3B^2 = 4p$ hat und den auch sonst schon bekannten Satz enthält, dass das Vierfache einer Primzahl von der Form $6\mu + 1$ sich als die Summe eines einfachen und eines dreifachen Quadrates darstellen lasse, auch dass sich unter diesen Formen von $4p$ mindestens eine befindet, wofür A die Form $3\alpha - 2$ und B die Form 3β mit ganzen Werthen von $\alpha = \frac{1}{3}(A + 2)$ und $\beta = \frac{1}{3}B$ hat.

Es gesellen sich mithin zu den übrigen Beziehungen ersten Grades noch die beiden

$$6\,2_3 - 3\,1_2 - 3\,1_3 - 2 = A = 3\alpha - 2 \text{ oder } 3\,2_3 - 1_2 - 1_3 = \alpha$$
$$3\,(1_2 - 1_3) = B = 3\beta \qquad\qquad 1_2 - 1_3 = \beta$$

wonach sich für die unbekannten Koeffizienten die Werthe

$$(35) \quad \begin{cases} 2_3 = \frac{1}{3}(\alpha + s) & 1_1 = \frac{1}{3}(\alpha + s - 3) \\ 1_2 = \frac{1}{6}(2s + 3\beta - \alpha) & 1_3 = \frac{1}{6}(2s - 3\beta - \alpha) \end{cases}$$

ergeben. Man sieht, dass hiernach die Koeffizienten für zulässige Werthe von $\pm A$ und $\pm B$ gebrochene Werthe annehmen könnten, was entschieden unzulässig ist, dass also nothwendig gewisse Werthe von α ausgeschlossen werden müssen; andererseits ist klar, dass ein Zeichenwechsel von B nur eine Vertauschung von 1_2 und 1_3 hervorbringt, also in allen Fällen zulässig ist, dass also immer eine paare Anzahl, mithin mindestens zwei mögliche Auflösungen in Betracht kommen. Im Übrigen leuchtet ein, dass wenn A ein zulässiger positiver oder negativer Werth ist, für welchen 2_3 und 1_3 ganz werden, — A kein zulässiger sein kann: denn es müsste zugleich $A + 2 + 3s$ und $-A + 2 + 3s$ durch 9 theilbar sein, folglich auch deren Summe $4 + 6s$, was offenbar nicht möglich ist. Da nun die Zerlegung von $4p$ nach Gl. (34) mit Werthen von A und B von der Form $3\alpha - 2$ und 3β nachweisbarermaassen nur in einziger Weise (abgesehen vom Zeichen von A und B) möglich ist; so ist klar, dass für die Koeffizienten stets zwei und auch nur zwei Auflösungen in Betracht kommen, worin jedoch die beiden Koeffizienten 2_3 und 1_1 bestimmte Werthe behalten und die beiden Koeffizienten 1_2 und 1_3 nur zwei bestimmte Werthe miteinander vertauschen können.

Da die Gl. (34) das Resultat einer geschickten Substitution ist; so ist es nützlich, die Gl. (33), welche von allen Koeffizienten unabhängig ist, etwas näher ins Auge zu fassen. Als quadratische Gleichung mit zwei Unbekannten von der allgemeinen Form

$$ax^2 + bxy + cy^2 + dx + ey = k$$

kann sie nach dem fünften Abschnitte meiner „Unbestimmten Analytik“ oder nach den Regeln meiner in Crelle's Journal Band 45 abge-

druckten Dissertation „Methodus nova aequationem indeterminatam secundi gradus duas incognitas implicantem per numeros integros solvendi" aufgelös't werden. Zu dem Ende ist dieselbe, da der Koeffizient des Gliedes $x\,y$ in Gl. (33) unpaar ist, nach zuvoriger Multiplikation mit 2, wodurch sie

$$6x^2 + 6xy + 6y^2 + [4 - 6(s-1)]x - 6(s-1)y = -2(s-1)(s-2)$$

wird, durch die Substitution (s. §. 125 meiner Unbestimmten Analytik)

$$x = \frac{X - 9(s-1) + 12}{-27} \qquad y = \frac{Y - 9(s-1) - 6}{-27}$$

in die Gleichung

$$X^2 + XY + Y^2 = 27(3s + 1) = 27p \tag{36}$$

überzuführen. Diese Formel lehrt, dass das 27-fache jeder Primzahl p von der Form $6\mu + 1$ in die Form $X^2 + XY + Y^2$ gebracht werden kann (so hat man z. B. für $p = 7$ $27 . 7 = 189 = 3^2 + 3 . 12 + 12^2$). Wegen der Beziehungen

$$X = -27x + 9(s-1) - 12 \qquad Y = -27y + 9(s-1) + 6$$

sind aber die Grössen X und Y durch 3 theilbar; es besteht also auch die Formel

$$A^2 + AB + B^2 = 3p \tag{37}$$

welche lehrt, dass das Dreifache jeder Primzahl von der Form $6\mu + 1$ in die Form $A^2 + AB + B^2$ gebracht werden kann (so ist z. B. für $p = 7$ $21 = 1^2 + 1 . 4 + 4^2$ und für $p = 13$ $39 = 2^2 + 2 . 5 + 5^2$).

Die Gl. (36) wird zwei Werthe für X und zu jedem derselben zwei Werthe von Y, also vier Auflösungen liefern. Man wird aber finden, dass von den beiden Werthen von X nur einer die Grösse x zu einer ganzen Zahl macht, welche den einzigen Werth des Koeffizienten 1_1 darstellt, während $y = 1_2$ zwei verschiedene Werthe annehmen kann. Die Einzigkeit des Werthes von x lässt sich konstatiren, wenn man die Gl. (27) einmal für $1_1 = x$ wie für eine einzige Unbekannte auflös't. Die Auflösung erscheint dann unter der Form

$$3x = -\frac{1}{2}[3y + 2 - 3(s-1)] \mp \frac{1}{2}\sqrt{K}$$

Durch einen zulässigen Werth von y muss K ein Quadrat werden und wenn Diess geschehen, muss $\sqrt{K}$ entweder $= 3w + 1$, oder $= 3w + 2$ sein, da der Werth $3w$ offenbar dieser Gleichung nicht genügen kann. Findet sich aber $\sqrt{K} = 3w + 1$; so muss die Wurzelgrösse negativ genommen werden, und findet sich $\sqrt{K} = 3w + 2$, so muss sie positiv genommen werden: immer kömmt für $x = 1_1$ nur ein einziger Werth in Betracht.

Aus dem Vorstehenden geht hervor, dass die beiden Koeffizienten 1_1 und 2_3 stets eindeutige Werthe haben, während die beiden Koeffizienten

1_2 und 1_3 zwei bestimmte vertauschbare Werthe besitzen, welche von der Beschaffenheit der primitiven Wurzel a abhängen.

Ferner geht hieraus hervor, dass für jede Primzahl von der Form $6\mu + 1$ eine paare Anzahl primitiver Wurzeln existiren, von welchen die Hälfte Perioden der einen Art und die andere Hälfte Perioden der anderen Art liefert.

18) Die Formeln (30), (31), (33) sind eine Quelle von gesetzlichen Beziehungen zwischen den Primzahlen p von der Form $6\mu + 1$ und den quadratischen Formen von der Gestalt $\delta X^2 + \delta' XY + \delta'' Y^2 = f(p)$. Ein besonderes Interesse haben stets diejenigen Funktionen $f(p)$ erweckt, welche sich in die quadratische Form $\delta X^2 + \delta' Y^2$ bringen lassen. Die vorhin erwähnte Beziehung $X^2 + 3Y^2 = 4p$ ist eine solche, und ich gestatte mir, über die rationelle Auffindung derselben folgende Bemerkungen zu machen. Angenommen, zwischen den beiden Unbekannten x, y sei die Gleichung

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$$

gegeben (die paaren Koeffizienten von x, y und xy können stets durch Multiplikation mit 2 hergestellt werden). Multiplizirt man die Gleichung mit n und addirt beiderseits die Zahl m; so kömmt

$$anx^2 + 2bnxy + cny^2 + 2dnx + 2eny + fn + m = m$$

Wenn diese Gleichung mit der Gleichung $\delta X^2 + \delta' Y^2 = m$ oder

$$\delta(\alpha x + \beta y + \gamma)^2 + \delta'(\alpha' x + \beta' y + \gamma')^2 = m$$

identisch sein soll; so müssen, nach Entwicklung der Quadrate auf der linken Seite, folgende Gleichungen bestehen

$$\delta\alpha^2 + \delta'\alpha'^2 = an \quad \delta\beta^2 + \delta'\beta'^2 = cn \quad \delta\gamma^2 + \delta'\gamma'^2 = fn + m$$
$$\delta\alpha\beta + \delta'\alpha'\beta' = bn \quad \delta\alpha\gamma + \delta'\alpha'\gamma' = dn \quad \delta\beta\gamma + \delta'\beta'\gamma' = en$$

Die dritte dieser 6 Gleichungen dient, nachdem die Grössen n, δ, δ', γ, γ' bekannt geworden sind, zur Bestimmung der Funktion

$$m = \delta\gamma^2 + \delta'\gamma'^2 - fn$$

man hat also 5 Gleichungen zur Bestimmung der 9 Unbekannten δ, δ', α, β, γ, α', β', γ', n in ganzen Zahlen.

Die drei Beziehungen, welche von γ und γ' unabhängig sind, dienen wesentlich zur Ermittlung der Werthe für n, α, β, α', β', δ, δ'. Für γ und γ' hat man alsdann wegen der letzten beiden der obigen 6 Bedingungen

$$\gamma = \frac{(d\beta' - e\alpha')n}{(\alpha\beta' - \alpha'\beta)\delta} \qquad \gamma' = -\frac{(d\beta - e\alpha)n}{(\alpha\beta' - \alpha'\beta)\delta'}$$

Diese beiden Gleichungen bestimmen γ und γ' direkt, sobald n, α, β, α', β', δ, δ' bekannt sind: für die letzteren Grössen enthalten sie aber noch die Forderung, dass γ und γ' ganze Zahlen werden.

Für die beiden Grössen δ und δ' können offenbar zwei relativ prime Zahlen (darunter jedoch auch ± 1 und ± 1 angenommen werden, da ein gemeinschaftlicher Theiler > 1 durch Division der Gleichung $\delta X^2 + \delta' Y^2 = m$ beseitigt werden kann. Ausserdem brauchen für δ und δ' nur solche Werthe zugelassen zu werden, welche keinen

quadratischen Faktor enthalten, da, wenn $\delta = \delta_1 \delta_2^2$ wäre, die Gleichung $\delta_1 (\delta_2 X)^2 + \delta' Y^2 = m$ alle Auflösungen der ersteren Gleichung mit enthält. Endlich kann immer $\delta = 1$ gesetzt werden, da sich die gegebene Gleichung durch Multiplikation mit δ in $(\delta X)^2 + \delta \delta' Y^2 = \delta m$ oder $X_1^2 + \delta_1 Y^2 = m_1$ verwandelt.

Aus den beiden Bedingungen

$$c (\delta \alpha^2 + \delta' \alpha'^2) = a (\delta \beta^2 - \delta' \beta'^2)$$
$$b (\delta \alpha^2 + \delta' \alpha'^2) = a (\delta \alpha \beta + \delta' \alpha' \beta')$$

folgt

$$\frac{\delta'}{\delta} = \frac{c \alpha^2 - a \beta^2}{a \beta'^2 - c \alpha'^2} = \frac{\alpha (b \alpha - a \beta)}{\alpha' (a \beta' - b \alpha')}$$

und sodann

$$c \alpha \alpha' + a \beta \beta' = b (\alpha \beta' + \alpha' \beta)$$

Diese quadratische Gleichung mit den vier Unbekannten $\alpha, \beta, \alpha', \beta'$, welche homogen ist und kein Quadrat der einen oder anderen enthält, kann nach §. 184 meiner Unbestimmten Analytik aufgelös't werden. Diese Auflösung ergiebt

$$\alpha = \frac{u}{c} \left\{ b v - \frac{(a c - b^2) v w}{t} \right\}$$
$$\alpha' = \frac{u}{c} (b w + t)$$
$$\beta = u v$$
$$\beta' = u w$$

Hierin sind u, v, w drei willkürliche Konstanten und t irgend ein Faktor von $(a c - b^2) v w$. Eine Substitution dieser Werthe in den Ausdruck für $\frac{\delta'}{\delta}$ giebt

$$\delta' = \frac{(a c - b^2) v^2 \delta}{t^2}$$

Da nun $\delta = 1$ ist und δ' keinen quadratischen Faktor enthalten soll; so hat man, wenn der ganze in $a c - b^2$ enthaltene quadratische Faktor h^2 und $a c - b^2 = h^2 i$ ist, $t = h v$ und $\delta' = i$ zu nehmen, d. h. die Grösse δ' kann nur dem positiven oder negativen Werthe des in $a c - b^2$ enthaltenen nichtquadratischen Faktors gleich sein. Wenn $a c - b^2$, resp. i positiv ist, haben δ und δ' gleiche Zeichen, δ' ist also positiv: wenn $a c = b^2$, resp. i negativ ist, haben δ und δ' entgegengesetzte Zeichen, δ' ist also negativ.

Für n muss sein in ganzen Zahlen

$$n = \frac{1}{a} (\delta \alpha^2 + \delta' \alpha'^2) = \frac{1}{c} (\delta \beta^2 + \delta' \beta'^2) = \frac{1}{b} (\delta \alpha \beta + \delta' \alpha' \beta')$$

Die vorstehenden Formeln sind von 4 Konstanten u, v, w, t abhängig, welche so zu wählen sind, dass alle 9 Unbekannten ganze Zahlen werden, welche aber im Übrigen willkürlich bleiben. Wendet man diese Formeln

auf Gl. (27) an, nachdem man dieselbe mit 2 multiplizirt hat, also, indem man $1_1 = x$ und $1_2 = y$ setzt, auf die Gleichung

$$6x^2 + 2.3xy + 6y^2 - 2(3s-5)x - 2.3(s-1)y + 2(s-1)(s-2) = 0$$

so ergiebt sich $ac - b^2 = 27 = 3^2.3$, also $h = 3$, $i = 3$ und demnach $\delta = 1$, $\delta' = 3$; man erkennt also sofort, dass die gegebene Gleichung nur in die quadratische Form $X^2 + 3Y^2$ gebracht werden kann. Hiernach ist

$$\alpha = \frac{u}{2}(v - 3w) \qquad \alpha' = \frac{u}{2}(v + w) \qquad \beta = uv \qquad \beta' = uw$$

$$n = \frac{u^2}{6}(v^2 + 3w^2) \qquad \frac{\alpha\beta' - \alpha'\beta}{n} = -3$$

$$\gamma = \frac{u}{6}[3(w-v)s + 3v - 7w] \qquad \gamma' = \frac{u}{18}[-3(v + 3w)s + 7v + 9w]$$

Die Werthe $u = 2$, $v = 0$, $w = 3$ machen alle diese Grössen zu ganzen Zahlen und man erhält hierfür $n = 18$, $\alpha = -9$, $\alpha' = 3$, $\beta = 0$, $\beta' = 6$, $\gamma = 3s - 7$, $\gamma' = -3(s-1)$, $m = 4(3s + 1) = 4p$, folglich an Stelle der Gleichung $X^2 + 3Y^2 = m$, wenn man X mit entgegengesetztem Zeichen nimmt,

$$[9\,1_1 - (3s - 7)]^2 + 3[3\,1_1 + 6\,1_2 - 3(s-1)]^2 = 4p$$

welche mit Gl. (34) übereinstimmt.

Wie die Zerlegung von $4p$ in Quadrate zur Bestimmung der Koeffizienten 1_1 und 1_2 dient, können, umgekehrt, die nach dem vorhergehenden Paragraphen aus den Resten der Potenzen einer primitiven Wurzel sich ergebenden Koeffizienten zur Zerlegung von $4p$ dienen. So hat man z. B. für $p = 73$

$P_1 =$ 1, 52, 3, 10, 9, 30, 27, 17, 8, 51, 24, 7, 72, 21,
70, 63, 64, 43, 46, 56, 65, 22, 49, 66

$P_2 =$ 5, 41, 15, 50, 45, 4, 62, 12, 40, 36, 47, 35, 68, 32,
58, 23, 28, 69, 11, 61, 33, 37, 26, 38

$P_3 =$ 25, 59, 2, 31, 6, 20, 18, 60, 54, 34, 16, 29, 48, 14,
71, 42, 67, 53, 55, 13, 19, 39, 57, 44

Um die Koeffizienten 1_0, 1_1, 1_2, 1_3 von $P_1 P_1$ zu bilden, addiren wir die Einheit zu jedem Reste von P_1, ebenso ergeben sich die Koeffizienten 2_0, 2_1, 2_2, 2_3 von $P_1 P_2$ durch Addition von 1 zu den Resten von P_2, endlich die Koeffizienten 3_0, 3_1, 3_2, 3_3 von $P_1 P_3$ durch Addition von 1 zu den Resten von P_3. Die erste Addition liefert ausser einem Nullreste 8 Reste aus P_1, 6 Reste aus P_2 und 9 Reste aus P_3. Die zweite Addition liefert 6 Reste aus P_1, 9 Reste aus P_2 und 9 Reste aus P_3. Die dritte Addition liefert 9 Reste aus P_1, 9 Reste aus P_2 und 6 Reste aus P_3; man hat also

$$P_1 P_1 = 1P_0 + 8P_1 + 6P_2 + 9P_3$$
$$P_1 P_2 = 6P_1 + 9P_2 + 9P_3$$
$$P_1 P_3 = 9P_1 + 9P_2 + 6P_3$$

Da $1_1 = 8$, $1_2 = 6$ und $s = 24$ ist; so ergiebt die Formel für $4p = 4 \cdot 73 = 292$ die Zerlegung $292 = 7^2 + 3 \cdot 9^2$.

19) Für $r = 4$ sind zur Bestimmung der 5 Unbekannten $1_1, 1_2, 1_3, 1_4, 2_3$ drei Gleichungen vorhanden; es fehlen also auch hier zwei Gleichungen. Die vierdimensionale Funktion

$$P_1 P_2 P_3 P_4 = \varrho_0 + \varrho_1 P_1 + \varrho_2 P_2 + \varrho_3 P_3 + P_4 P_4$$

liefert die Beziehungen

$$\varrho_1 = \varrho_2 = \varrho_3 = \varrho_4 = \frac{1}{4}(s^3 - \varrho_0)$$

worunter sich jedoch identische befinden. Die drei Gleichungen (26) sind

$$\begin{aligned} 1_0 + 1_1 + 1_2 + 1_3 + 1_4 &= s \\ 2_0 + 2_1 + 2_2 + 2_3 + 2_4 &= s \\ 3_0 + 3_1 + 3_2 + 3_3 + 3_4 &= s \end{aligned}$$

Für ein paares s werden diese Gleichungen nach der Koeffiziententafel in Nr. 6

$$\begin{aligned} 1_1 + 1_2 + 1_3 + 1_4 &= s - 1 \\ 1_2 + 1_4 + 2 \cdot 2_3 &= s \\ 2\,(1_3 + 2_3) &= s \end{aligned}$$

Die Koeffizienten ϱ sind

$$\begin{aligned}
\varrho_0 = {} & 4_0\,2_1\,3_1 + 4_0\,2_2\,2_4 + 4_0\,2_3\,1_3 + 4_0\,2_4\,4_2 \\
& + 3_0\,2_1\,3_2 + 3_0\,2_2\,2_1 + 3_0\,2_3\,1_4 + 3_0\,2_4\,4_3 \\
+ 2_0\,2_0\,s & + 2_0\,2_1\,3_3 + 2_0\,2_2\,2_2 + 2_0\,2_3\,1_1 + 2_0\,2_4\,4_4 \\
& + 1_0\,2_1\,3_4 + 1_0\,2_2\,2_3 + 1_0\,2_3\,1_2 + 1_0\,2_4\,4_1 \\
\varrho_1 = {} & 4_1\,2_1\,3_1 + 4_1\,2_2\,2_4 + 4_1\,2_3\,1_3 + 4_1\,2_4\,4_2 \\
& + 3_4\,2_1\,3_2 + 3_4\,2_2\,2_1 + 3_4\,2_3\,1_4 + 3_4\,2_4\,4_3 \\
+ 2_3\,2_0\,s & + 2_3\,2_1\,3_3 + 2_3\,2_2\,2_2 + 2_3\,2_3\,1_1 + 2_3\,2_4\,4_4 \\
& + 1_2\,2_1\,3_4 + 1_2\,2_2\,2_3 + 1_2\,2_3\,1_2 + 1_2\,2_4\,4_1 \\
\varrho_2 = {} & 4_2\,2_1\,3_1 + 4_2\,2_2\,2_4 + 4_2\,2_3\,1_3 + 4_2\,2_4\,4_2 \\
& + 3_1\,2_1\,3_2 + 3_1\,2_2\,2_1 + 3_1\,2_3\,1_4 + 3_1\,2_4\,4_3 \\
+ 2_4\,2_0\,s & + 2_4\,2_1\,3_3 + 2_4\,2_2\,2_2 + 2_4\,2_3\,1_1 + 2_4\,2_4\,4_4 \\
& + 1_3\,2_1\,3_4 + 1_3\,2_2\,2_3 + 1_3\,2_3\,1_2 + 1_3\,2_4\,4_1 \\
\varrho_3 = {} & 4_3\,2_1\,3_1 + 4_3\,2_2\,2_4 + 4_3\,2_3\,1_3 + 4_3\,2_4\,4_2 \\
& + 3_2\,2_1\,3_2 + 3_2\,2_2\,3_1 + 3_2\,2_3\,3_4 + 3_2\,2_4\,3_3 \\
+ 2_1\,2_0\,s & + 2_1\,2_1\,3_3 + 2_1\,2_2\,3_2 + 2_1\,2_3\,3_1 + 2_1\,2_4\,3_4 \\
& + 1_4\,2_1\,3_4 + 1_4\,2_2\,3_3 + 1_4\,2_3\,3_2 + 1_4\,2_4\,3_1 \\
\varrho_4 = {} & (2_1\,3_0 + 2_2\,2_0 + 2_3\,1_0 + 2_4\,4_0)\,s \\
& + 4_4\,2_1\,3_1 + 4_4\,2_2\,2_4 + 4_4\,2_3\,1_3 + 4_4\,2_4\,4_2 \\
& + 3_3\,2_1\,3_2 + 3_3\,2_2\,2_1 + 3_3\,2_3\,1_4 + 3_3\,2_4\,4_3 \\
+ 2_2\,2_0\,s & + 2_2\,2_1\,3_3 + 2_2\,2_2\,2_2 + 2_2\,2_3\,1_1 + 2_2\,2_4\,4_4 \\
& + 1_1\,2_1\,3_4 + 1_1\,2_2\,2_3 + 1_1\,2_3\,1_2 + 1_1\,2_4\,4_1
\end{aligned}$$

Vermöge der Koeffiziententafel und da für ein paares s $2_0 = 3_0 = 4_0 = 0$ und $1_0 = 1$ ist, wird

$$\varrho_0 = 1_2\,2_3 + 1_4\,2_3 + 2_3\,1_2 + 2_3\,1_4 = 2\,.\,2_3\,(1_2 + 1_4)$$

$$\begin{aligned}\varrho_1 = {} & 1_4\,1_2\,1_3 + 1_4\,1_4\,2_3 + 1_4\,2_3\,1_3 + 1_4\,2_3\,2_3 \\ & + 2_3\,1_2\,2_3 + 2_3\,1_4\,1_2 + 2_3\,2_3\,1_4 + 2_3\,2_3\,2_3 \\ & + 2_3\,1_2\,1_3 + 2_3\,1_4\,1_4 + 2_3\,2_3\,1_1 + 2_3\,2_3\,1_2 \\ & + 1_2\,1_2\,2_3 + 1_2\,1_4\,2_3 + 1_2\,2_3\,1_2 + 1_2\,2_3\,1_4\end{aligned}$$

$$\begin{aligned}\varrho_2 = {} & 2_3\,1_2\,1_3 + 2_3\,1_4\,2_3 + 2_3\,2_3\,1_3 + 2_3\,2_3\,2_3 \\ & + 1_3\,1_2\,2_3 + 1_3\,1_4\,1_2 + 1_3\,2_3\,1_4 + 1_3\,2_3\,2_3 \\ & + 2_3\,1_2\,1_3 + 2_3\,1_4\,1_4 + 2_3\,2_3\,1_1 + 2_3\,2_3\,1_2 \\ & + 1_3\,1_2\,2_3 + 1_3\,1_4\,2_3 + 1_3\,2_3\,1_2 + 1_3\,2_3\,1_4\end{aligned}$$

$$\begin{aligned}\varrho_3 = {} & 2_3\,1_2\,1_3 + 2_3\,1_4\,2_3 + 2_3\,2_3\,1_3 + 2_3\,2_3\,2_3 \\ & + 2_3\,1_2\,2_3 + 2_3\,1_4\,1_2 + 2_3\,2_3\,1_4 + 2_3\,2_3\,2_3 \\ & + 1_2\,1_2\,1_3 + 1_2\,1_4\,1_4 + 1_2\,2_3\,1_1 + 1_2\,2_3\,1_2 \\ & + 1_4\,1_2\,2_3 + 1_4\,1_4\,2_3 + 1_4\,2_3\,1_2 + 1_4\,2_3\,1_4\end{aligned}$$

$$\begin{aligned}\varrho_4 = {} & 2_3\,s + 1_2\,1_2\,1_3 + 1_2\,1_4\,2_3 + 1_2\,2_3\,1_3 + 1_2\,2_2\,2_3 \\ & + 1_3\,1_2\,2_3 + 1_3\,1_4\,1_2 + 1_3\,2_3\,1_4 + 1_3\,2_3\,2_3 \\ & + 1_4\,1_2\,1_3 + 1_4\,1_4\,1_4 + 1_4\,2_3\,1_1 + 1_4\,2_3\,1_2 \\ & + 1_1\,1_2\,2_3 + 1_1\,1_4\,2_3 + 1_1\,2_3\,1_2 + 1_1\,2_3\,1_4\end{aligned}$$

Die Gleichung $\varrho_1 = \varrho_2$ führt zu der Beziehung

$$(1_2 + 1_4 - 2\,.\,1_3)\,(2\,.\,1_2 + 1_4 + 2_3) = 0$$

welche, da nach den drei Gleichungen ersten Grades $1_2 + 1_4 - 2\,.\,1_3 = 0$ ist, eine Identität darstellt, also nichts Neues aussagt.

Die Gleichung $\varrho_1 = \varrho_3$ liefert, wenn man 1_1, 1_4, 2_3 eliminirt,

$$1_2^3 + 5\,1_3^3 - 1_2^2\,1_3 + 3\,1_2\,1_3^2 - \frac{1}{2}\,s\,1_2^2 - \frac{1}{2}\,(9s-2)\,1_3^2 - (s-1)\,1_2\,1_3$$
$$+ \frac{1}{4}\,s\,(s-2)\,1_2 + \frac{1}{4}\,s\,(5s-4)\,1_3 - \frac{1}{8}\,s^2\,(s-2) = 0\,.$$

Die Gleichung $\varrho_1 = \varrho_4$ dagegen

$$1_2^3 - 35\,1_3^3 - 9\,1_2^2\,1_3 + 19\,1_2\,1_3^2 + \frac{1}{2}\,3\,s\,1_2^2 + \frac{1}{2}\,(43\,s-14)\,1_3^2$$
$$-(5s-1)\,1_2\,1_3 + \frac{1}{4}\,s\,(s-2)\,1_2 - \frac{1}{4}\,s\,(19s-20)\,1_3 + \frac{3}{8}\,s^2\,(s-2) = 0$$

Die Gleichung $\varrho_3 = \varrho_4$ ergiebt

$$1_2^3 - 15\,1_3^3 - 5\,1_2^2\,1_3 + 11\,1_2\,1_3^2 + \frac{1}{2}\,s\,1_2^2 + \frac{1}{2}\,(17s-6)\,1_3^2 - (3s-1)\,1_2\,1_3$$
$$+ \frac{1}{4}\,s\,(s-2)\,1_2 - \frac{1}{4}\,s\,(7s-8)\,1_3 + \frac{1}{8}\,s^2\,(s-2) = 0$$

Die Existenz von drei selbstständigen Gleichungen zwischen zwei Unbekannten würde die nach dem vorhergehenden Paragraphen offenbar mögliche Aufgabe unmöglich machen, und die Existenz von zwei selbstständigen Gleichungen würde die durch die Änderung der primitiven Wurzel eine mehrfache Auflösung zulassende, also unbestimmte Aufgabe zu einer bestimmten machen. Da Beides einen Widerspruch involviren würde; so müssen jene drei Gleichungen entweder einander äquivalent sein, oder sie müssen gemeinschaftliche Wurzeln enthalten. Die Abhängigkeit der dritten von den anderen beiden Gleichungen ergiebt sich auch sofort durch Addition der ersten beiden Gleichungen.

20) Es kann die Vermuthung entstehen, dass sich die vorstehende Gleichung mit 2 Unbekannten $1_2 = x$ und $1_3 = y$, welche (nöthigenfalls durch Multiplikation mit 6) in die Form

$$g x^3 + 3hx^2y + 3ixy^2 + ky^3 + 3ax^2 + 6bxy + 3cy^2 + 3dx + 3ey + f = F = 0$$

gebracht werden kann, nach Multiplikation mit einer Zahl n und Hinzufügung einer Grösse m nicht in der kubischen Form

$$\delta X^3 + \delta' Y^3 = m$$

worin m eine Funktion von s, also auch von der Primzahl p bezeichnet, dargestellt werden könne. Zur Erfüllung dieser Form müsste

$$X = \alpha x + \beta y + \gamma \qquad Y = \alpha' x + \beta' x + \gamma'$$

sein, und es kann stets $\delta = 1$ gesetzt und für δ' eine positive Zahl, welche keinen kubischen Faktor hat, gedacht werden. Eine Substitution der Werthe X und Y in die angenommene Form und eine Identifikation des Resultates mit $nF + m$ ergiebt folgende 10 Bedingungsgleichungen

$$\begin{array}{lll}
\delta\alpha^3 + \delta'\alpha'^3 = gn & \delta\beta^3 + \delta'\beta'^3 = kn & \delta\gamma^3 + \delta'\gamma'^3 = fn+m \\
\delta\alpha^2\beta + \delta'\alpha'^2\beta' = hn & \delta\alpha\beta^2 + \delta'\alpha'\beta'^2 = in & \\
\delta\alpha^2\gamma + \delta'\alpha'^2\gamma' = an & \delta\beta^2\gamma + \delta'\beta'^2\gamma' = cn & \delta\alpha\beta\gamma + \delta'\alpha'\beta'\gamma' = bn \\
\delta\alpha\gamma^2 + \delta'\alpha'\gamma'^2 = dn & \delta\beta\gamma^2 + \delta'\beta'\gamma'^2 = en &
\end{array}$$

Durch Division von je zwei der vier Gleichungen, welche kein γ und γ' enthalten, ergeben sich Beziehungen für das Verhältniss von δ' und δ in Ausdrücken wie

$$\frac{\delta'}{\delta} = \frac{k\alpha^3 - g\beta^3}{g\beta'^3 - k\alpha'^3} = \frac{g\beta^2 - i\alpha^2}{i\alpha'^2 - g\beta'^2} \cdot \frac{\alpha}{\alpha'} = \frac{h\alpha - g\beta}{g\beta' - h\alpha'} \cdot \frac{\alpha^2}{\alpha'^2}$$
$$= \frac{i\alpha - h\beta}{\beta' - i\alpha'} \cdot \frac{\alpha\beta}{\alpha'\beta'} = \frac{h\beta^2 - k\alpha^2}{k\alpha'^2 - h\beta'^2} \cdot \frac{\beta}{\beta'}$$

Diese Beziehungen führen zu den beiden Gleichungen

$$i\alpha\alpha' + g\beta\beta' = h(\alpha\beta' + \alpha'\beta)$$
$$k\alpha\alpha' + h\beta\beta' = i(\alpha\beta' + \alpha'\beta)$$

und diese zu der Gleichung

$$\frac{\alpha\alpha'}{\beta\beta'} = \frac{gi - h^2}{hk - i^2}$$

Ebenso führen die drei Bedingungen, welche a, b, c enthalten, zu der Gleichung

$$c\,\alpha\,\alpha' + a\,\beta\,\beta' - b\,(\alpha\,\beta' + \alpha'\,\beta)$$

welche mit den vorstehenden Gleichungen die Relation

$$\frac{\alpha\,\alpha'}{\beta\,\beta'} = \frac{b\,g - a\,h}{c\,h - b\,i} = \frac{b\,h - a\,i}{c\,i - b\,k}$$

ergiebt. Hiernach müsste zwischen den gegebenen Grössen g, h, i, k, a, b, c eine bestimmte Beziehung, welche sich auch in die Form

$$a\,(h\,k - i^2) + b\,(h\,i - g\,k) + c\,(g\,i - h^2) = 0$$

bringen lässt, bestehen. Diese Beziehung besteht aber zwischen den Koeffizienten unserer Gleichung nicht: denn diese Gleichung ist nach Multiplikation mit 6

$$6x^3 + 3(-2)x^2y + 3\,.\,6xy^2 + 30y^3 + 3(-s)x^2 + 6(-s+1)xy$$
$$+ 3(-9s+2)y^2 + 3\,.\,\frac{s(s-2)}{2}x + 3\,\frac{s(5s-4)}{2}y + \left(-\frac{3s^2(s-2)}{4}\right) = 0$$

und die vorhergehende Beziehung würde verlangen, dass

$$-s(-96) + (-s+1)(-192) + (-9s+2)\,32 = -128 = 0$$

sei. Aus dieser Analyse ergiebt sich der allgemeine Satz, dass es keine ganzzahlige Funktion der Primzahlen $p = 8\mu + 1$ geben kann, welche sich allgemein als die Summe eines einfachen und eines mehrfachen Kubus oder überhaupt in der Form $\delta X^3 + \delta' Y^3$ darstellen lässt. Dass eine Darstellung als Summe von mehr als zwei Vielfachen von Kuben überhaupt nicht in Betracht kommen kann, leuchtet ebenfalls ein, da Diess zwischen den beiden Unbekannten x und y drei Gleichungen ergeben würde, was für eine als möglich erkannte Aufgabe unmöglich ist.

21) Die beiden aus $\varrho_1 = \varrho_3$ und $\varrho_1 = \varrho_4$ hervorgehenden Gleichungen sind offenbar nicht äquivalent, müssen also, da sie gemeinschaftliche Auflösungen haben und nur zwei Variabelen enthalten, einen gemeinschaftlichen Faktor vom ersten oder vom zweiten Grade haben, es muss sich also die linke Seite einer jeden in das Produkt

$$(x + \alpha' y + \beta')\,(x^2 + \alpha\,x\,y + \beta\,y^2 + \gamma\,x + \delta\,y + \varepsilon)$$

zerlegen lassen. (Ein nur von y abhängiger Rest, welcher $= 0$ zu setzen wäre, kann hier nicht in Betracht kommen, da hierdurch die Aufgabe zu einer bestimmten gemacht werden würde). Führt man die Multiplikation aus und identifizirt die einzelnen Glieder mit den gleich dimensionirten Gliedern der ersten gegebenen Gleichung; so kömmt

$$\alpha + \alpha' = -1 \qquad \beta + \alpha\,\alpha' = 3 \qquad \alpha'\,\beta = 5$$

$$\gamma + \beta' = -\frac{1}{2}s \qquad \delta + \alpha\beta' + \alpha'\gamma = -s + 1 \qquad \alpha'\delta + \beta\beta' = -\frac{1}{2}(9s - 2)$$

$$\varepsilon+\beta'\gamma=\frac{1}{4}s(s-2) \quad \alpha'\varepsilon+\beta'\delta=-\frac{1}{4}(5s-4) \quad \beta'\varepsilon=-\frac{1}{8}s^2(s-2)$$

und hieraus folgt

$$\alpha'=1 \quad \beta'=-\frac{1}{2}s \quad \alpha=-2 \quad \beta=5 \quad \gamma=0$$

$$\delta=-(2s-1) \quad \varepsilon=\frac{1}{4}s(s-2)$$

Hiernach hat man für die erste gegebene Gleichung

$$\left(x+y-\frac{s}{2}\right)\left\{x^2-2xy+5y^2-(2s-1)y+\frac{s(s-2)}{4}\right\}=0$$

Die zweite gegebene Gleichung fordert

$$\alpha+\alpha'=-9 \quad \beta+\alpha\alpha'=19 \quad \alpha'\beta=-35$$

$$\gamma+\beta'=\frac{3}{2}s \quad \delta+\alpha\beta'+\alpha'\gamma=-5s+1 \quad \alpha'\delta+\beta\beta'=\frac{1}{2}(43s-14)$$

$$\varepsilon+\beta'\gamma=\frac{1}{4}s(s-2) \quad \alpha'\varepsilon+\beta'\delta=-\frac{1}{4}s(19s-20) \quad \beta'\varepsilon=\frac{3}{8}s^2(s-2)$$

und hieraus folgt

$$\alpha'=-7 \quad \beta'=\frac{3}{2}s \quad \alpha=-2 \quad \beta=5$$

$$\gamma=0 \quad \delta=-(2s-1) \quad \varepsilon=\frac{1}{4}s(s-2)$$

mithin statt der zweiten Gleichung

$$\left(x-7y+\frac{3s}{2}\right)\left\{x^2-2xy+5y^2-(2s-1)y+\frac{s(s-2)}{4}\right\}=0$$

In den auf diese Weise gewonnenen Formen sind die linearen Faktoren ungleich, enthalten also nicht die gemeinschaftlichen Auflösungen: dagegen sind die beiden Faktoren zweiten Grades einander gleich; die gemeinschaftlichen Wurzeln der gegebenen kubischen Gleichungen sind mithin die Auflösungen der quadratischen Gleichung

$$x^2-2xy+5y^2-(2s-1)y+\frac{s(s-2)}{4}=0$$

Wenn man (um den Koeffizienten von y zu einer paaren Zahl zu machen) mit 2 multiplizirt, ergiebt die Substitution

$$x=-\frac{X-2(2s-1)}{16} \quad y=-\frac{Y-2(2s-1)}{16}$$

$$2X^2-4XY+10Y^2=32(4s+1)=32p$$

oder

$$X^2-2XY+5Y^2=16p$$

oder auch, wenn man $X-Y-2Z$ setzt,

$$Z^2+Y^2=4p$$

Diese Formel enthält den Satz, dass sich das Vierfache einer jeden Primzahl von der Form $8\mu + 1$ als die Summe zweier Quadrate darstellen lässt. Da x und y ganze Zahlen, also X, Y und Z paare Zahlen sein müssen; so fällt vorstehender Satz auch mit dem Satze $Z'^2 + Y'^2 = p$ zusammen, welcher als bekannt anzusehen ist, da jede Primzahl von der Form $8\mu + 1$ auch der Form $4\nu + 1$ angehört.

Alle diejenigen Zerlegungen von p in Y und Z, welche für $X = Y + 2Z$ und $Y = Y$ die beiden Grössen

$$x = -\frac{Y + Z - 2(2s-1)}{16} \qquad y = -\frac{Y - 2(2s-1)}{16}$$

zu ganzen Zahlen machen (wobei Y und Z für sich nach Belieben positiv oder negativ genommen werden können) liefern eine Auflösung, d. h. sie ergeben zulässige Werthe für $x = 1_2$ und $y = 1_3$, aus welchen alsdann für die übrigen drei Koeffizienten $1_1 = s = 1 - 3\,1_3$, $1_4 = 2\,1_3 - 1_2$, $2_3 = \frac{1}{2}s - 1_3$ folgt. Beispielsweise hat man für $p = 73 = 4 \cdot 18 + 1$, weil $4 \cdot 73 = 292 = (\pm 6)^2 + (\pm 16)^2$ ist, die beiden Auflösungen $1_2 = 2$, $1_3 = 4$ und $1_2 = 6$, $1_3 = 4$.

22) Bei der Berechnung der Koeffizienten für die Primzahlen $p = 4s + 1$, worin s unpaar ist, beachte man, dass nach der Schlussbemerkung in Nr. 7 die allgemeinen Formeln (welche noch alle Koeffizienten in ursprünglicher Bezeichnung enthalten) in die gesuchten übergehen, wenn man 1_0 und 3_0, ferner 1_1 und 1_3, ferner 1_2 und 1_4, ferner 2_3 und 2_1 miteinander vertauscht (die Vertauschung von 1_2 und 1_4 kann in diesem speziellen Falle auch unterbleiben). Die Gleichungen (26) werden jetzt

$$\begin{aligned} 1_1 + 1_2 + 1_3 + 1_4 &= s \\ 1_2 + 1_4 + 2 \cdot 2_1 &= s \\ 2(1_1 + 2_1) &= s - 1 \end{aligned}$$

und die Koeffizienten der Kombination $P_1\,P_2\,P_3\,P_4$ liefern jetzt nach der Absonderung des gemeinschaftlichen Faktors die quadratische Gleichung

$$5x^2 - 2xy + y^2 - 2(s-2)x - y + \frac{(s-1)(s-3)}{4} = 0$$

worin $x = 1_1$ und $y = 1_4$ ist. Nachdem diese Gleichung mit 2 multiplizirt ist, ergiebt die Substitution

$$x = -\frac{X - 2(2s-3)}{16} \qquad y = -\frac{Y - 2(2s+1)}{16}$$

die Gleichung

$$5X^2 - 2XY + Y^2 = 16p$$

oder, wenn man $X - Y = 2Z$ setzt,

$$Z^2 + X^2 = 4p$$

Hiernach lässt sich auch das Vierfache einer Primzahl von der Form $8\mu + 5$ als die Summe zweier Quadrate darstellen. Hat man durch die letzte Gleichung zulässige Werthe für 1_1 und 1_4 bestimmt; so ergeben sich die übrigen Koeffizienten durch die Beziehungen $1_2 = 1 + 2 \cdot 1_1 - 1_4$, $1_3 = s - 1 - 3 \cdot 1_1$, $2_1 = \frac{1}{2}(s-1) - 1_1$.

23) Das vorstehende Verfahren zur Bestimmung der Koeffizienten ist völlig allgemein und lässt sich auch in allgemeinen Zeichen ausführen. Denn zunächst ergiebt sich nach den Regeln in Nr. 6 und 7 für jeden Werth von r und s die vollständige Koeffiziententafel in generellen Zeichen, sowie die Anzahl der darin unbekannt bleibenden Koeffizienten. Alsdann liefert Nr. 11 $m + 1$ Beziehungen zwischen diesen unbekannten Koeffizienten. Hierzu stellt die Nr. 14 vermöge der r gleichen Koeffizienten $\varrho_1, \varrho_2, \ldots \varrho_r$ der Kombination $P_1 P_2 \ldots P_r$ noch $r-1$ Gleichungen vom Grade $r-1$, und wir heben hervor, dass diese Funktion $P_1 P_2 \ldots P_r$ als lineare Funktion $\varrho_0 P_0 + \varrho_1 P_1 + \varrho_2 P_2 + \ldots$ der Grössen $P_0, P_1, P_2 \ldots$ nur durch sukzessive Multiplikation einer zweidimensionalen Kombination wie $P_1 P_2$ mit den einzelnen Grössen $P_3, P_4 \ldots P_r$ unter Substitution der Werthe für $P_1 P_1$, $P_1 P_2$, $P_1 P_3$ etc. nach Nr. 5 hergestellt werden darf, wenn man sicher sein will, in der Endgleichung nicht lauter identische Werthe für $\varrho_1, \varrho_2, \ldots \varrho_r$ zu erhalten, dass also z. B. für $r = 4$ das Produkt $P_1 P_2 P_3 P_4$ nicht durch das Produkt aus $P_1 P_2$ und $P_3 P_4$ oder aus $P_1 P_3$ und $P_2 P_4$, d. h. aus Faktoren, von welchen irgend einer die zyklische Verschiebung eines anderen ist, erzeugt werden darf.

Nach dieser Regel ergeben sich also $m + r$ Bedingungsgleichungen, welche den Inbegriff aller möglichen Bedingungen darstellen. Wenn vermittelst der ersten $m + 1$ Bedingungen $m + 1$ Koeffizienten durch die übrigen ausgedrückt und ihre Werthe in die letzten $r - 1$ Gleichungen substituirt werden; so hat man $r - 1$ Gleichungen vom Grade $r - 1$ mit einer bestimmten Anzahl von Unbekannten. Jede Auflösung in ganzen Zahlen, welche alle diese $r - 1$ Gleichungen zusammen erfüllt, entspricht einer Auflösung der gestellten Aufgabe: es handelt sich also um die gemeinschaftlichen Auflösungen eines Systems von Gleichungen. Zur Bewirkung derselben hat man diejenigen Gleichungen, welche gewisse Unbekannte ausschliesslich enthalten, für sich zu betrachten: angenommen also (A) sei eine Gruppe dieser Gleichungen, von welchen keine Unbekannte in einer anderen Gleichung erscheint, und (B), (C) etc. seien andere Gruppen dieser Art. Da die Gruppen (A), (B), (C) ... in keiner Beziehung zueinander stehen; so entspricht jede gemeinschaftliche Auflösung der Gruppe (A) mit jeder beliebigen gemeinschaftlichen Auflösung der Gruppe (B) mit jeder beliebigen gemeinschaftlichen Auflösung der Gruppe (C) u. s. w. den Bedingungen der Aufgabe, und es kömmt nur darauf an, eine Gruppe von Gleichungen wie (A), (B), (C) ... für sich aufzulösen.

Die ganze Aufgabe kann nur eine endliche Menge von Auflösungen in lauter positiven Zahlen, welche $\leq s$ sind, haben. Die Anzahl der Auflösungen lehrt, wie viel verschiedene Grundtafeln von Resten mit r Horizontalreihen sich durch die verschiedenen

primitiven Wurzeln a bilden lassen, wobei alle diejenigen Tafeln als gleich erscheinen, welche in denselben Horizontalreihen dieselben Reste, unbekümmert um deren Reihenfolge, enthalten.

Durch dieses Verfahren ist die Bestimmung der Koeffizienten in allgemeinen Zeichen auf ganz bestimmte Regeln gebracht, welche von den Werthen p, r, s unabhängig sind. Mir däucht, dass darin eine wesentliche Ergänzung der bisherigen Theorie der Kreistheilung zu erblicken sei.

Als besonderes Resultat der obigen Betrachtungen führen wir noch an, dass die aus der Gleichheit der in der Kombination $P_1 P_2 \ldots P_r$ enthaltenen Koeffizienten $\varrho_1, \varrho_2 \ldots \varrho_r$ sich ergebenden Gleichungen stets allgemeine Eigenschaften gewisser Funktionen der Primzahlen p von der Form $rs + 1$ nicht allein für ein paares, sondern auch für ein unpaares, also für jedes s darstellen, was auf der in Nr. 7 erwähnten Beziehung zwischen den Koeffiziententafeln für ein paares und unpaares s beruhet.

24) Die thatsächliche Zerlegung der kubischen Gleichung für $r = 4$ in einen linearen und einen quadratischen Faktor, welcher letztere das gemeinschaftliche Maass aller gefundenen kubischen Gleichungen ist, veranlasst uns, die Aufgabe unter dem Gesichtspunkte zu prüfen, ob die niedrigsten Gleichungen nicht direkt darstellbar seien.

In der That, stellt man für $r = 4$ die dreidimensionale Kombination $P_1 P_2 P_3$ einmal in der Weise her, dass man $P_1 P_2$ mit P_3 multiplizirt, und einmal in der Weise, dass man $P_1 P_3$ mit P_2 multiplizirt; so ergiebt sich

$$\begin{aligned}
P_1 P_2 P_3 = {} & 2_3 P_0 + (2_1 3_1 + 2_2 2_4 + 2_3 1_3 + 2_4 2_3) P_1 \\
& + (2_1 3_2 + 2_2 2_1 + 2_3 1_4 + 2_4 2_4) P_2 \\
& + (2_1 3_3 + 2_2 2_2 + 2_3 1_1 + 2_4 2_1) P_3 \\
& + (2_1 3_4 + 2_2 2_3 + 2_3 1_2 + 2_4 2_2) P_4 \\
P_1 P_3 P_2 = {} & 3_2 P_0 + (3_1 2_1 + 3_2 1_4 + 3_3 2_4 + 3_4 3_4) P_1 \\
& + (3_1 2_2 + 3_2 1_1 + 3_3 2_1 + 3_4 3_1) P_2 \\
& + (3_1 2_3 + 3_2 1_2 + 3_3 2_2 + 3_4 3_2) P_3 \\
& + (3_1 2_4 + 3_2 1_3 + 3_3 2_3 + 3_4 3_3) P_4
\end{aligned}$$

Setzt man die Koeffizienten von P_0, P_1, P_2, P_3, P_4 aus diesen beiden Gleichungen einander gleich und substituirt für $1_1, 1_2, 1_4, 2_3$ die obigen Ausdrücke, welche sich aus den linearen Beziehungen ergeben; so zeigt sich, dass die beiden Koeffizienten von P_1, sowie die beiden von P_4 identisch sind, dass aber sowohl die Koeffizienten von P_2, als auch die von P_3 die quadratische Gleichung

$$1_3^2 - 2\, 1_2\, 1_3 + 5\, 1_3^2 - (2s - 1)\, 1_3 + \frac{s(s-2)}{4} = 0$$

ergeben, welche mit der in Nr. 21 durch das gemeinschaftliche Maass der aus dem Werthe von $P_1 P_2 P_3 P_4$ gewonnenen kubischen Gleichungen hergestellten Gleichung übereinstimmt.

Es ist leicht zu übersehen, dass für jeden beliebigen Werth von r die dreidimensionale Kombination $P_1 P_2 P_3$, wenn sie einmal als das Produkt $P_1 P_2 \times P_3$ und einmal als das Produkt $P_1 P_3 \times P_2$ gebildet wird, quadratische Gleichungen, ferner die vierdimensionale Kombination $P_1 P_2 P_3 P_4$ kubische, die fünfdimensionale Kombination

biquadratische Gleichungen zwischen den obigen Koeffizienten ergiebt, wenn man eine solche Kombination nach verschiedener Reihenfolge der Faktoren bildet und die daraus entstehenden Koeffizienten der gleichnamigen Grössen P einander gleich setzt. Von den Gleichungen desselben Grades erweisen sich einige identisch, wenn darin für $m + 1$ Unbekannte ihre aus den linearen Grundgleichungen sich ergebenden Werthe substituirt werden; die übrig bleibenden Gleichungen können gemeinschaftliche Faktoren enthalten und müssen sich nach Absonderung dieser Faktoren immer, da die Aufgabe eine mögliche ist und nur eine endliche Menge von Auflösungen zulässt, auf eine bestimmte Anzahl selbstständiger Gleichungen reduziren. Eine jede solche Gleichung stellt eine bestimmte Funktion einer Primzahl p von gegebener Form $rs + 1$ als einen Ausdruck von bestimmtem Grade zwischen variabelen Zahlen dar, welche Letzteren zwar noch unbekannt sind, von welchen man aber weiss, dass sie ganz sind; eine solche Gleichung bildet also die Darstellung einer ganzzahligen Funktion einer Primzahl in quadratischer, kubischer, biquadratischer oder höherer Form. Durch Substitution linearer Ausdrücke für die Variabelen können aus einer solchen Gleichung n-ten Grades die Glieder von erster Potenz beseitigt und dadurch die in Rede stehende Funktion der Primzahl p in eine einfachere Form n-ten Grades gebracht werden, und häufig wird sich die entstehende Gleichung, besonders wenn sie keiner Zerlegung in Faktoren mehr fähig ist, in die noch einfachere Form

$$a A^n + b B^n + c C^n + \text{etc.} = f(p)$$

welche die Zerlegung von $f(p)$ in eine Summe von n-ten Potenzen darstellt, oder doch in die Form

$$a_0 A_0^n + b_0 B_0^n + \text{etc.} + a_1 A_1^{n-1} + b_1 B_1^{n-1} + \text{etc.} + \ldots + a_{n-2} A_{n-2}^2 + b_{n-2} B_{n-2}^2 = f_1(p)$$

welche die Zerlegung in eine Summe von 2., 3., 4. . . . n-ten Potenzen darstellt, bringen lassen. Unter Umständen wird sich die in Rede stehende Funktion $f(p)$ auf ein einfaches Vielfaches von p reduziren lassen, zuweilen ist Diess jedoch nicht möglich.

Da die Grössen $A, B \ldots A_1, B_1 \ldots A_2, B_2 \ldots A_{n-2}, B_{n-2}$ lineare Ausdrücke der Unbekannten von der Form $\alpha x + \beta y + \gamma z + \ldots$ sind; so kann, weil die Aufgabe eine mögliche ist, die Anzahl der durch diese Zerlegungen entstehenden selbstständigen Gleichungen $\alpha x + \beta y + \gamma z + \ldots = A$, $\alpha' x + \beta' y + \gamma' z + \ldots = B$ etc. nicht grösser werden, als die Zahl der Unbekannten $x, y, z \ldots$ Fände man also eine grössere Anzahl; so hätte man damit zugleich Beziehungen zwischen den Grössen $A, B \ldots A_1, B_1 \ldots A_2, B_2 \ldots$ gewonnen.

Eine Anwendung des Vorstehenden auf den Fall $r = 5$, welcher ein paares s, also Primzahlen von der Form $10\mu + 1$ voraussetzt, ergiebt zunächst die in Nr. 6 mitgetheilte Koeffiziententafel mit den 7 Unbekannten $1_1, 1_2, 1_3, 1_4, 1_5, 2_3, 2_4$ und den drei linearen Gleichungen

$$1_1 + 1_2 + 1_3 + 1_4 + 1_5 = s - 1$$
$$1_2 + 1_5 + 2 \cdot 2_3 + 2_4 = s$$
$$1_3 + 1_4 + 2_3 + 2 \cdot 2_4 = s$$

wodurch sich 3 Unbekannte durch die 4 übrigen ausdrücken lassen. Bildet man die Kombination $P_1 P_2 P_3$ einmal durch die Multiplikation von $P_1 P_2$ mit P_3 und einmal durch die Multiplikation von $P_1 P_3$ mit P_2; so ergeben sich durch Ausgleichung der Faktoren der Grössen P_1, P_2, P_3, P_4, P_5 fünf Gleichungen. Die erste Gleichung erweis't sich ohne Weiteres als eine Identität; die vierte, sowie die fünfte Gleichung wird durch Substitution der Werthe für 3 Unbekannte eine Identität; die zweite Gleichung zeigt sich als eine selbstständige und mit der dritten übereinstimmende Beziehung. Eliminirt man daraus die 3 Unbekannten $1_5, 2_3, 2_4$; so wird sie

$$16\,1_1^2 + 9\,1_2^2 + 9\,1_3^2 + 18\,1_4^2 + 9\,1_1\,1_2 + 30\,1_1\,1_3 + 39\,1_1\,1_4 + 18\,1_2\,1_4 + 27\,1_3\,1_4 - 2(11s - 13)\,1_1 - 9(s-1)\,1_2 - 3(5s-7)\,1_3 - 6\,(4s-5)\,1_4 + (7s-5)\,(s-2) = 0$$

Stellt man in ähnlicher Weise die Kombination $P_1 P_2 P_4$ einmal als das Produkt $P_1 P_2 \times P_4$ und einmal als das Produkt $P_1 P_4 \times P_2$ dar; so giebt die Gleichsetzung der Koeffizienten von P_1, sowie die der Koeffizienten von P_3 und die der Koeffizienten von P_5 je eine identische Gleichung. Aus den Koeffizienten von P_2 aber erhält man die neue Gleichung

$$5\,1_1^2 - 18\,1_3^2 - 9\,1_4^2 + 3\,1_1\,1_3 + 12\,1_1\,1_4 - 9\,1_2\,1_3 + 9\,1_2\,1_4 - 18\,1_3\,1_4 - (5s-7)\,1_1 + 6\,(2s-1)\,1_3 + 3\,(s+1)\,1_4 - (s+1)\,(s-2) = 0$$

Wie die dreidimensionale Kombination quadratische Formeln liefert; so lassen sich mit Hülfe der vierdimensionalen Kombination kubische und mit Hülfe der fünfdimensionalen Kombination biquadratische Gleichungen für die Primzahlen von der Form $10\mu + 1$ aufstellen.

25) Wenn alle Koeffizienten $1_1, 1_2 \ldots 2_1, 2_2 \ldots$ etc. bekannt geworden sind, lassen sich die Werthe aller zyklischen Perioden $F(P_\alpha P_\beta P_\gamma \ldots)$ leicht darstellen. Man braucht zu dem Ende, wenn eine solche Periode aus mehreren primitiven zyklischen Reihen besteht, nur von dem Anfangsgliede einer jeden Reihe, welches die Form

$$P_\alpha P_\beta P_\gamma \ldots = \varphi_0 P_0 + \varphi_1 P_1 + \varphi_2 P_2 + \ldots$$

hat, den Koeffizienten φ_0 darzustellen, um daraus nach Nr. 9 sofort den Werth der zyklischen Reihe zu bilden.

Die eindimensionale Funktion ist stets $F(P_1) = -1$.

Für $r = 2$ und ein paares s, also für die Primzahlen $p = 4\mu + 1$ ist die zweidimensionale Kombination $P_1 P_2 = 2_1 P_1 + 2_2 P_2 +$ etc., also $\varphi_0 = 0$, folglich nach Gl. (23)

$$F(P_1 P_2) = P_1 P_2 = -\frac{s}{2} = -\frac{p-1}{4}$$

Für $r = 2$ und ein unpaares s, also für $p = 4\mu + 3$ ist $\varphi_0 = 1$, mithin nach Gl. (23)

$$F(P_1 P_2) = P_1 P_2 = \frac{1}{2}(p - s) = \frac{1}{2}(s + 1) = \frac{p+1}{4}$$

Die quadratische Gleichung, deren Wurzeln die Grössen P sind, ist hiernach für ein paares s

$$x^2 + x - \frac{p-1}{4} = 0$$

und für ein unpaares s

$$x^2 + x + \frac{p+1}{4} = 0$$

Für $r = 3$, was ein paares s, also Primzahlen von der Form $p = 6\mu + 1$ voraussetzt, ist $P_1 P_2 = 2_1 P_1 + 2_2 P_2 +$ etc., also $\varphi_0 = 0$ und daher nach Gl. (20)

$$F(P_1 P_2) = -s = -\frac{p-1}{3}$$

Ferner ist in $P_1 P_2 P_3 = \varphi_0 P_0 + \varphi_1 P_1 +$ etc. nach Nr. 13 $\varphi_0 = 2_1 3_0 + 2_2 2_0 + 2_3 1_0 = 2_3$, mithin nach Gl. (23)

$$F(P_1 P_2 P_3) = \frac{1}{3}(p\, 2_3 - s^2) = \frac{1}{3}\left[p\, 2_3 - \left(\frac{p-1}{3}\right)^2\right]$$

und die kubische Gleichung, deren Wurzeln die Werthe von P_1, P_2, P_3 ergeben, ist

$$x^3 + x^2 - \frac{p-1}{3}x - \frac{1}{3}\left[2_3\, p - \left(\frac{p-1}{3}\right)^2\right] = 0$$

Durch Substitution des Werthes $\frac{1}{3}(\alpha + s)$ für 2_3 nach den Gleichungen (35) vereinfacht sich das konstante Glied dieser Gleichung auf $-\left[p\,\alpha + \frac{p-1}{3}\right]$.

Für $r = 4$ besteht die zweidimensionale symmetrische Funktion aus zwei primitiven Reihen $P_1 P_2 + P_2 P_3 + P_3 P_4 + P_4 P_1$ und $P_1 P_3 + P_2 P_4$. Für ein paares s ist sowohl für das erste Glied $P_1 P_2$ der ersten Reihe, als auch für das erste Glied $P_1 P_3$ der zweiten Reihe $\varphi_0 = 0$. Da die erste Reihe aus $r = 4$ Gliedern besteht; so hat diese Reihe nach Gl. (20) den Werth $-s$.

Die zweite Reihe besteht aus $r' = 2$ Gliedern und hat daher nach Gl. (22) den Werth $-\frac{1}{2}s$, sodass die ganze zweidimensionale Funktion $F = -\frac{3}{2}s$ ist.

In der dreidimensionalen Kombination $P_1 P_2 P_3$ ist nach Nr. 25 $\varphi_0 = 2_3$, folglich hat die dreidimensionale symmetrische Funktion selbst wegen Gl. (20) den Werth $2_3\, p - s^2$.

In der vierdimensionalen Kombination $P_1 P_2 P_3 P_4$, welche zugleich die symmetrische Funktion ist, ist nach Nr. 19 und 20 $\varphi_0 = 2 \cdot 2_3(1_2 + 1_4) = 4\, 1_3\, 2_3$, mithin hat diese Funktion selbst nach Gl. (23) den Werth $\frac{1}{4}(4\, 1_3\, 2_3\, p - s^3)$. Hiernach ist die biquadratische Gleichung, deren Wurzeln die Werthe von P_1, P_2, P_3, P_4 ergeben, für ein paares s

$$x^4 + x^3 - \frac{3s}{2} x^2 - (2_3 p - s^2) x + \frac{1}{4} (4\, 1_3\, 2_3\, p - s^3) = 0$$

worin $s = \frac{p-1}{4}$ und nach Nr. 21 $1_3 = \frac{1}{2} s - 2_3$ ist, sodass diese Gleichung nur von dem einen Koeffizienten 2_3 oder 1_3, dessen Werth sich aus Nr. 21 ergiebt, abhängig erscheint.

Für ein unpaares s bleibt in dem Ausdrucke für $P_1 P_2$ $\varphi_0 = 0$, in dem Ausdrucke für $P_1 P_3$ wird dagegen $\varphi_0 = 1$, und man erhält für die erste symmetrische Reihe nach Gl. (20) den Werth $-s$ und für die zweite, nur aus 2 Gliedern bestehende Reihe nach Gl. (22) den Werth $\frac{1}{2}(p - s)$, für beide also die zweidimensionale Funktion

$$F_2 = \frac{1}{2} (p - 3s) = \frac{1}{2} (s + 1)$$

Die dreidimensionale Funktion wird $2_1 p - s^2$ und die vierdimensionale $\frac{1}{4} [(1_2^2 + 1_4^2 + 2 \cdot 2_1^2) p - s^3]$, die biquadratische Gleichung also

$$x^4 + x^2 + \frac{1}{2}(s+1) x^2 - (2_1 p - s^2) x + \frac{1}{4}[(1_2^2 + 1_4^2 + 2 \cdot 2_1^2) p - s^3] = 0$$

Für $r = 5$ besteht die zweidimensionale Funktion aus zwei primitiven Reihen von je 5 Gliedern, deren erste das Anfangsglied $P_1 P_2$ und deren zweite das Anfangsglied $P_1 P_3$ hat. Für beide ist $\varphi_0 = 0$ und daher nach Gl. (25)

$$F_2 = -\frac{5 \cdot 4}{1 \cdot 2} \cdot \frac{s}{5} = -2s = -\frac{2(p-1)}{5}$$

Die dreidimensionale Funktion besteht ebenfalls aus zwei primitiven Reihen, deren erste Glieder resp. $P_1 P_2 P_3$ und $P_1 P_2 P_4$ sind. Für die erste Reihe ist $\varphi_0' = 2_3$ und für die zweite Reihe $\varphi_0'' = 2_4$; man hat also nach Gl. (25)

$$F_3 = (2_3 + 2_4) p - \frac{5 \cdot 4 \cdot 3}{1 \cdot 2 \cdot 3} \cdot \frac{s^2}{5} = (2_3 + 2_4) p - 2 s^2$$

Die vierdimensionale Funktion besteht aus einer primitiven Reihe, deren erstes Glied $P_1 P_2 P_3 P_4$ ist. Man hat hierfür

$$\varphi_0 = 2_1 3_4 + 2_2 2_3 + 2_3 1_2 + 2_4 2_2 + 2_5 3_2 = (1_2 + 1_5)(2_3 + 2_4) + 2_3^2$$

folglich nach Gl. (25)

$$F_4 = [(1_2 + 1_5)(2_3 + 2_4) + 2_3^2] p - \frac{5 \cdot 4 \cdot 3 \cdot 2}{1 \cdot 2 \cdot 3 \cdot 4} \cdot \frac{s^3}{5}$$

$$= [(1_2 + 1_5)(2_3 + 2_4) + 2_3^2] p - s^3$$

Für die fünfdimensionale Funktion hat man nach Gl. (23)

$$F_5 = \frac{1}{5} \varphi_0 p - \frac{s^4}{5}$$

worin $\varphi_0 =$

$$\begin{aligned}
&4_5\,(2_1\,3_1 + 2_2\,2_5 + 2_3\,1_4 + 2_4\,2_4 + 2_5\,3_4)\\
&+ 3_4\,(2_1\,3_2 + 2_2\,2_1 + 2_3\,1_5 + 2_4\,2_5 + 2_5\,3_5)\\
&+ 2_3\,(2_1\,3_3 + 2_2\,2_2 + 2_3\,1_1 + 2_4\,2_1 + 2_5\,3_1)\\
&+ 1_2\,(2_1\,3_4 + 2_2\,2_3 + 2_3\,1_2 + 2_4\,2_2 + 2_5\,3_2)\\
&+ 2_2\,(2_1\,3_5 + 2_2\,2_4 + 2_3\,1_3 + 2_4\,2_3 + 2_5\,3_3)\\
=\;&2_3\,(1_2\,1_3 + 1_5\,2_3 + 2_3\,1_4 + 2_4\,2_4 + 2_3\,2_4)\\
&+ 2_4\,(1_2\,2_3 + 1_5\,1_2 + 2_3\,1_5 + 2_4\,2_5 + 2_3\,2_4)\\
&+ 2_3\,(1_2\,1_4 + 1_5\,1_5 + 2_3\,1_1 + 2_4\,1_2 + 2_3\,1_3)\\
&+ 1_2\,(1_2\,2_4 + 1_5\,2_3 + 2_3\,1_2 + 2_4\,1_5 + 2_3\,2_3)\\
&+ 1_5\,(1_2\,2_4 + 1_5\,2_4 + 2_3\,1_3 + 2_4\,2_3 + 2_3\,1_4)
\end{aligned}$$

ist. Die Gleichung fünften Grades, deren Wurzeln die Grössen P_1, P_2, P_3, P_4, P_5 darstellen, ist hiernach

$$x^5 + x^4 - 2s\,x^3 - [(2_3 + 2_4)\,p - 2s^2]\,x^2$$
$$+ \left\{[(1_2 + 1_5)\,(2_3 + 2_4) + 2_3^{\,2}]\,p - s^3\right\} x - \left(\frac{\varphi_0}{5}\,p - \frac{s^4}{5}\right) = 0$$

Wenn man für einen beliebigen primen oder nichtprimen Werth von r in der Finalgleichung $s = \frac{p-1}{r}$ substituirt, nimmt diese Gleichung die Form

$$(r\,x + 1)^r + (a_{r-2}\,x^{r-2} + a_{r-3}\,x^{r-3} + \ldots + a_1\,x + a_0)\,p = 0$$

an, in welcher das in die $(r-1)$-te Potenz der Unbekannten multiplizirte Glied fehlt, sobald man $r\,x + 1 = y$ setzt, welche also, wenn r den Werth 4 nicht übersteigt, zur sofortigen Auflösung geeignet ist.

26) Für den Werth $r = p - 1$ wird $s = 1$; die Reihen $P_1, P_2 \ldots P_r$ enthalten sämmtlich nur einen Rest, also jede eine der Zahlen $1, 2, 3 \ldots r$. Hiernach kann auch jede der Kombinationen $P_1 P_1$, $P_1 P_2$, $P_1 P_3 \ldots P_1 P_r$ nur aus einem einzigen Gliede mit dem Koeffizienten 1 bestehen. Die Kombination $P_1 P_{\frac{r}{2}}$ ist stets $= 1 \,.\, P_0$, d. h. es ist der Koeffizient $\left(\frac{r}{2}\right)_0 = 1$ und jeder der Koeffizienten $\left(\frac{r}{2}\right)_1, \left(\frac{r}{2}\right)_2 \ldots \left(\frac{r}{2}\right)_r$ ist $= 0$. In jeder anderen Koeffizientenreihe $1_1, 1_2 \ldots 1_r$ oder $2_1, 2_2 \ldots 2_r$ oder $3_1, 3_2 \ldots 3_r$ ist einer $= 1$ und alle übrigen sind $= 0$. Kennt man irgend einen dieser Koeffizienten, welcher $= 1$ ist; so ergiebt sich daraus nach den in Nr. 7 aufgestellten Regeln die ganze Koeffiziententafel. Da nach diesen Regeln die vertikale Reihe $1_1, 2_1, 3_1 \ldots r_1$ die Koeffizienten

$$\left(\frac{r}{2}\right)_1, \left(\frac{r}{2}\right)_2, \left(\frac{r}{2}\right)_3 \cdots \left(\frac{r}{2}\right)_r$$

aufnimmt; so sind alle erst genannten Koeffizienten $= 0$. Nimmt man also nach und nach $1_2 = 1$, später $1_3 = 1$, dann $1_4 = 1$ u. s. f.; so lassen sich leicht alle möglichen Koeffiziententafeln für eine gegebene Primzahl p aufstellen, indem einige dieser Annahmen auf Widersprüche

führen, da sie verlangen, dass in irgend einer horizontalen Reihe mehr als ein Koeffizient = 1 werde. So erhält man z. B. für $p = 5$, $r = 4$ die mögliche Koeffiziententafel

	Koeffiziententafel	entspr. der Resttafel
$P_1 P_1 =$	$0 P_1 + 0 P_2 + 0 P_3 + 1 P_4$	1
$P_1 P_2 =$	$0 P_1 + 0 P_2 + 1 P_3 + 0 P_4$	3
$P_1 P_3 = 1 P_0 +$	$0 P_1 + 0 P_2 + 0 P_3 + 0 P_4$	4
$P_1 P_4 =$	$0 P_1 + 1 P_1 + 0 P_3 + 0 P_4$	2

welche aus der primitiven Wurzel $a = 3$ hervorgeht; man kann aber auch folgende Tafel bilden

	Koeffiziententafel	entspr. der Resttafel
$P_1 P_1 =$	$0 P_1 + 1 P_2 + 0 P_3 + 0 P_4$	1
$P_1 P_2 =$	$0 P_1 + 0 P_2 + 0 P_3 + 1 P_4$	2
$P_1 P_3 = 1 P_0 +$	$0 P_1 + 0 P_2 + 0 P_3 + 0 P_4$	4
$P_1 P_4 =$	$0 P_1 + 0 P_2 + 1 P_3 + 0 P_4$	3

welche aus der primitiven Wurzel 2 hervorgeht.

Für $r = p - 1$ muss sich die in Nr. 25 betrachtete Gleichung r-ten Grades, deren Wurzeln die Werthe der Perioden P_1, $P_2 \ldots P_r$ sind, nothwendig auf

$$x^r + x^{r-1} + x^{r-2} + \ldots + x + 1 = 0$$

reduziren, was sich für $p = 3$ durch die dortige quadratische Gleichung und für $p = 5$ durch die dortige biquadratische Gleichung für ein ungerades s auch vollkommen bestätigt, da in der letzteren $2_1 = 0$ und $1_2^2 + 1_4^2$ für jede der beiden möglichen Koeffiziententafeln = 1 ist.

27) Die in Nr. 25 aufgestellte Periodengleichung r-ten Grades, deren Wurzeln die aus s-gliedrigen Perioden der Reste bestehenden Grössen P_1, P_2, $\ldots$ P_r sind, ist in einer von der primitiven Wurzel a, nach welcher die Grundtafel der Reste aufgestellt ist, ganz unabhängigen Weise abgeleitet, insbesondere sind die in Nr. 11 aufgestellten Bedingungsgleichungen ersten Grades für die Koeffizienten $1_0, 1_1, 1_2 \ldots 2_0, 2_1, 2_2 \ldots$ etc. von der Wurzel a unabhängig. Ergäben also verschiedene Auflösungen der unbestimmten Gleichungen, welche die Bedingungsgleichungen so weit ergänzen, dass daraus alle eben genannten Koeffizienten bestimmt werden können, verschiedene Werthe für die Koeffizienten der Periodengleichung; so erhielte man mehrere solche Gleichungen, also auch mehrere Systeme der r Grössen P, welches auch der spezielle Werth der primitiven Wurzel a sein möge. Nun liefert aber ein bestimmter Werth von a nach §. 5 nur ein einziges System von Perioden P, und daraus folgt, dass die Periodengleichung ebenfalls nur ein einziges System solcher Grössen liefern kann, dass also ihre Koeffizienten (für eine gegebene Primzahl p) ganz bestimmte, von der primitiven Wurzel a unabhängige Werthe haben müssen, dass also eine einzige Auflösung der obigen unbestimmten Gleichungen zur Bestimmung der Koeffizienten der Periodengleichung ausreicht.

Die Besonderheit der Wurzel a beeinflusst nur die Werthe der Koeffizienten $1_0, 1_1, 1_2 \ldots, 2_0, 2_1, 2_2 \ldots$ etc. und in weiterer Folge die Stellung der Reste in den einzelnen Perioden $P_1, P_2 \ldots P_r$, sowie endlich die Reihenfolge dieser Grössen P, nicht aber den Werth jedes einzelnen P, wenn dasselbe nur als ein Inbegriff von Resten ohne Rücksicht auf deren Stellung betrachtet wird. Da die Koeffizienten der Periodengleichung die symmetrischen Funktionen der Grössen P darstellen; so erweisen sich alle diese Funktionen unabhängig von der primitiven Wurzel a.

Die Periodengleichung liefert durch ihre Wurzeln die Werthe aller r Grössen P, sagt aber Nichts über deren Reihenfolge aus, worüber wir im nächsten Paragraphen Betrachtungen anstellen werden.

Um die Konstanz der Koeffizienten der Periodengleichung bei Veränderung der primitiven Wurzel a an dem Beispiele $p = 31 = 5 \cdot 6 + 1$ für $r = 5$, $s = 6$ zu zeigen; so erhält man für die primitiven Wurzeln $a = 3$ und $a = 11$ die beiden Grundtafeln

	für $a = 3$						für $a = 11$					
$P_1 =$	1	26	25	30	5	6	1	6	5	30	25	26
$P_2 =$	3	16	13	28	15	18	11	4	24	20	27	7
$P_3 =$	9	17	8	22	14	23	28	13	16	3	18	15
$P_4 =$	27	20	24	4	11	7	29	19	21	2	12	10
$P_5 =$	17	29	10	12	2	21	9	23	14	22	8	17

also die Koeffiziententafeln

für $a = 3$

$$
\begin{aligned}
P_1 P_1 &= 1 P_0 + 2 P_1 + 0 P_2 + 0 P_3 + 2 P_4 + 1 P_5 \\
P_1 P_2 &= \quad 0 P_1 + 1 P_2 + 2 P_3 + 1 P_4 + 2 P_5 \\
P_1 P_3 &= \quad 0 P_1 + 2 P_2 + 2 P_3 + 1 P_4 + 1 P_5 \\
P_1 P_4 &= \quad 2 P_1 + 1 P_2 + 1 P_3 + 0 P_4 + 2 P_5 \\
P_1 P_5 &= \quad 1 P_1 + 2 P_2 + 1 P_3 + 2 P_4 + 0 P_5
\end{aligned}
$$

für $a = 11$

$$
\begin{aligned}
P_1 P_1 &= 1 P_0 + 2 P_1 + 2 P_2 + 0 P_3 + 1 P_4 + 0 P_5 \\
P_1 P_2 &= \quad 2 P_1 + 0 P_2 + 1 P_3 + 2 P_4 + 1 P_5 \\
P_1 P_3 &= \quad 0 P_1 + 1 P_2 + 1 P_3 + 2 P_4 + 2 P_5 \\
P_1 P_4 &= \quad 1 P_1 + 2 P_2 + 2 P_3 + 0 P_4 + 1 P_5 \\
P_1 P_5 &= \quad 0 P_1 + 1 P_2 + 2 P_3 + 1 P_4 + 2 P_5
\end{aligned}
$$

Sowohl nach der einen, wie nach der anderen Koeffiziententafel wird die Gleichung 5. Grades aus Nr. 25, deren Wurzeln die Grössen P_1, P_2, P_3, P_4, P_5 sind,

$$x^5 + x^4 - 12 x^3 - 21 x^2 + x + 5 = 0$$

§. 7. Die vollständige Auflösung.

1) Durch die Formeln des vorhergehenden Paragraphen werden die Werthe der Perioden P_1, P_2, P_3 ... gewonnen, welche die r-gliedrigen Horizontalreihen der Grundtafel der Reste darstellen. Diese Operation entspricht der Zerlegung des Exponenten $p-1$ in die r Faktoren $s = \frac{p-1}{r}$. Die vollständige Auflösung erfordert aber die Bestimmung jedes einzelnen der $p-1$ Reste der Grundtafel, also zunächst die weitere Zerlegung des Exponenten s in seine Faktoren. Formirt man zu diesem Ende eine Horizontalreihe P zur einer partiellen Tafel, indem man $s = r's'$ setzt und aus dieser Tafel r' Reihen mit je s' Gliedern bildet (also die ersten r' Glieder von P zu den ersten Gliedern von ebenso viel Horizontalreihen, sodann die folgenden r' Glieder von P zu den zweiten Gliedern dieser Reihen u. s. w. nimmt); so behalten alle Relationen, welche nach dem vorigen Paragraphen zwischen den Horizontalreihen und der ganzen Grundtafel bestehen, für die Horizontalreihen der eben erwähnten partiellen Tafel und einer anderen partiellen Gesammttafel Gültigkeit, d. h. die Kombinationen der Horizontalreihen der gedachten partiellen Grundtafel von bestimmter Dimensität bewegen sich in einer bestimmten Anzahl der anderen partiellen Tafeln und füllen dieselbe bei zyklischer Verschiebung vollständig aus: es kömmt nur darauf an, für jede gegebene Dimensität jener Kombinationen die Partialtafeln, welche davon berührt werden, zu ermitteln. Zu dem Ende ist aber die Kenntniss der Gesammtheit der Werthe, welche die Grössen $P_1, P_2 \ldots P_r$ in willkürlicher Reihenfolge anzunehmen vermögen und wie sie durch die Wurzeln der im vorigen Paragraphen in Nr. 25 aufgestellten Gleichungen r-ten Grades gefunden werden, durchaus nicht ausreichend; es kömmt vielmehr wesentlich noch auf die Ermittlung der Reihenfolge an, in welcher jene Wurzeln die einzelnen Grössen $P_1, P_2 \ldots$ zu vertreten vermögen: erst hierdurch sind die Einzelwerthe dieser Grössen bestimmt.

2) Wir wollen zunächst den einfachsten Fall ins Auge fassen, wo $r = p-1$, $s = 1$ ist, wo also die Grundtafel der Reste aus r eingliedrigen Reihen besteht. Diese Reste sind dann die Reste der sukzessiven Potenzen einer primitiven Wurzel a, also kongruent den Potenzen $a^0, a^1, a^2 \ldots a^{r-1}$ nach dem Model $p = r+1$, und sie enthalten in irgend einer Reihenfolge die Zahlen 1, 2, 3 ... r.

Diese Reste sind die symbolischen Vertreter der Wurzeln der Gleichung $x^p - 1 = 0$ nach Ausschluss der reellen Wurzel 1, also die Vertreter der Wurzeln der Gleichung

$$(38) \qquad \frac{x_p - 1}{x - 1} = x^r + x^{r-1} + x^{r-2} + \ldots + x + 1 = 0$$

Die Grössen $P_1, P_2 \ldots P_r$ sind diese Wurzeln selbst, sie sind also die Einheitswurzeln vom Grunde p mit Ausschluss der reellen Wurzel 1, also die $p-1 = r$ komplexen Einheitswurzeln. Ist ϱ_1 die dem kleinsten Winkel $\varphi = \frac{2\pi}{p}$ entsprechende Wurzel

$$\varrho_1 = e^{\frac{2\pi}{p} i} = cos\ \frac{2\pi}{p} + sin\ \frac{2\pi}{p} \cdot i$$

welche wir die erste nennen wollen; so ist die n-te Wurzel

$$\varrho_n = e^{\frac{2n\pi}{p} i} = cos\ \frac{2n\pi}{p} + sin\ \frac{2n\pi}{p} \cdot i \tag{39}$$

Eine Auflösung der gegebenen Gleichung r-ten Grades würde nun r Werthe ergeben, welche diesen r komplexen Einheitswurzeln gleich sind, ohne eine bestimmte Reihenfolge zu kennzeichnen.

Bei der zyklischen Form der Tafel der Reste und der Grössen P leuchtet nun ein, dass man allgemein, selbst wenn r ein beliebiger Faktor von $p-1$ oder $p = rs + 1$ ist, jede beliebige der s-gliedrigen Grössen $P_1, P_2 \ldots P_r$ zur ersten annehmen oder gleich P_1 setzen kann. Wenn Diess geschehen, kann nicht mehr jede beliebige andere für P_2 angenommen werden; es sind vielmehr nur gewisse Reihenfolgen möglich (welche den verschiedenen Werthen der primitiven Wurzeln a entsprechen). Wenn eine einzige Reihenfolge bekannt ist, ergeben sich daraus alle diejenigen, welche mit demselben Anfangsgliede beginnen, folgendermaassen. Angenommen, $P_1, P_2, P_3, \ldots P_r$ sei eine mögliche Reihenfolge. Aus den im vorigen Paragraphen nachgewiesenen Eigenschaften der Grössen P ist klar, dass wenn man in der Reihe $P_1, P_2, P_3 \ldots P_r$ von dem ersten Gliede P_1 in gleichen Intervallen zyklisch fortschreitet, also z. B. die Reihenfolge $P_1, P_3, P_5 \ldots$ bildet, indem man nach dem letzten Gliede P_r auf das erste P_1 übergeht, mithin P_{r+1} in P_1 verwandelt, eine mögliche Reihenfolge von Horizontalreihen oder von Grössen P entsteht, vorausgesetzt, dass durch diese zyklische Bewegung sämmtliche r Grössen $P_1, P_2 \ldots P_r$ getroffen werden, was die Rückkehr zur ersten nach sich zieht, aber die mehrmalige Wiederkehr derselben Grösse vor der Vollendung von r Sprüngen ausschliesst. Setzt man also die Differenz zwischen den Zeigern zweier benachbarten P gleich a; so ergiebt

$$P_1,\ P_{1+a},\ P_{1+2a} \ldots P_{1+(r-1)a}$$

eine mögliche Reihenfolge, wenn die Differenz a eine zu r relativ prime Zahl ist.

Hiernach sind ebenso viel verschiedene Reihenfolgen der Grössen P mit demselben Anfangsgliede P_1 möglich, als es relativ prime Zahlen zu r giebt, welche kleiner als r sind. Diese Reihenfolgen entsprechen den verschiedenen primitiven Wurzeln der Kongruenz $x^r \equiv 1 \ mod\ p$, und es ergiebt sich hieraus der bekannte Satz über die Anzahl der primitiven Wurzeln dieser Kongruenz. Andererseits aber erkennt man daraus, dass wenn $r = p - 1$ ist, jede primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \ mod\ p$ eine besondere Reihenfolge der P, also eine besondere Grundtafel bedingt.

Da $p-1$ eine paare Zahl ist; so kann für $r = p-1$ die Differenz a nicht $= 2$ sein: es kann also $P_1, P_3, P_5 \ldots$ keine zulässige Reihenfolge sein. (Für einen unpaaren Werth von r würde allerdings $a = 2$ sein können.)

Aus Vorstehendem folgt, dass man jede beliebige der r Wurzeln der

obigen Gleichung r-ten Grades, also irgend eine der Grössen $\varrho_1, \varrho_2, \ldots \varrho_r$, welche wir mit ϱ bezeichnen wollen, für die erste Periode P_1 annehmen, also, wenn a eine primitive Wurzel der Kongruenz $x^r \equiv 1 \; mod \; p$ ist,

$$P_1 = \varrho = \varrho^{a^0}, \quad P_2 = \varrho^a = \varrho^{a^1}, \quad P_3 = \varrho^{a^2}, \quad P_4 = \varrho^{a^3}, \ldots \; P_r = \varrho^{a^{r-1}}$$

setzen, d. h. durch Erhebung der Grösse ϱ zu Potenzen vom Grade $a, a^2, a^3 \ldots a^{r-1}$ oder auch zu Potenzen vom Grade $b_1, b_2, b_3 \ldots b_{r-1}$, womit die kleinsten Reste von $a, a^2, a^3 \ldots a^{r-1}$ bezeichnet sind, die Grössen $P_2, P_3 \ldots P_r$ in richtiger Reihenfolge bilden oder die gegebenen Grössen P o r d n e n kann.

Hat man z. B. für $p = 5$, $r = 4$ die vier Wurzeln der biquadratischen Gleichung $x^4 + x^3 + x^2 + x + 1 = 0$ gefunden und ist ϱ irgend eine derselben; so kann man, da 3 eine primitive Wurzel von $x^4 \equiv 1 \; mod \; 5$ und $3^2 \equiv 4$, $3^3 \equiv 2$ ist,

$$P_1 = \varrho, \quad P_2 = \varrho^3, \quad P_3 = \varrho^{3^2} = \varrho^4, \quad P_4 = \varrho^{3^3} = \varrho^2$$

man kann auch, da 3 relativ prim zu 4 ist, für $a = 3$

$$P_1 = \varrho, \quad P_2 = \varrho^{3^3} = \varrho^2, \quad P_3 = \varrho^{3^6} = \varrho^{3^2} = \varrho^4, \quad P_4 = \varrho^{3^9} = \varrho^3$$

man kann aber nicht, da 2 ein gemeinschaftliches Maass mit 4 hat, $a = 2$, also nicht

$$P_1 = \varrho, \quad P_2 = \varrho^{2^2} = \varrho^4, \quad P_3 = \varrho^{2^4} = \varrho^1, \quad P_4 = \varrho^{2^6} = \varrho^4$$

nehmen, indem in der letzteren Periode die Grössen ϱ^1 und ϱ^4 zweimal wiederkehren.

3) Die Annahme irgend eines beliebigen ϱ, welches das ϱ_n sein mag, für das erste ϱ_1 ist gleichbedeutend mit der Substitution von $(\varrho_1)^n$ für ϱ_1, und hierdurch verwandeln sich, wenn $b_1, b_2, b_3 \ldots$ die kleinsten Reste von $a^0, a^1, a^2 \ldots$ und wenn $c_1, c_2, c_3 \ldots$ die kleinsten Reste von $n b_1, n b_2, n b_3 \ldots$ sind,

die Grössen	ϱ_1	ϱ_2	ϱ_3	.	.	.	
welche gleich	ϱ_1^1	ϱ_1^2	ϱ_1^3	.	.	.	sind,
in	ϱ_1^n	ϱ_1^{2n}	ϱ_1^{3n}	.	.	.	
oder in	ϱ_n	ϱ_{2n}	ϱ_{3n}	.	.	.	
und es verwandeln sich							
die Grössen	ϱ_{b_0}	ϱ_{b_1}	ϱ_{b_2}	.	.	.	
welche gleich	$\varrho_1^{b_0}$	$\varrho_1^{b_1}$	$\varrho_1^{b_2}$	.	.	.	sind,
in	$\varrho_1^{n\,b_0}$	$\varrho_1^{n\,b_1}$	$\varrho_1^{n\,b_2}$	.	.	.	
oder in	$\varrho_1^{c_0}$	$\varrho_1^{c_1}$	$\varrho_1^{c_2}$	.	.	.	
oder in	ϱ_{c_0}	ϱ_{c_1}	ϱ_{c_2}	.	.	.	

4) Nehmen wir jetzt $r = \frac{p-1}{2}$, $s = 2$, sodass es sich um r zweigliedrige Perioden handelt; so ist für jede primitive Wurzel a $a^r \equiv -1$,

also der Rest von a^r gleich $p-1$, und demnach ist die erste Periode $P_1 = \varrho_1 + \varrho_{p-1} = \varrho_1 + \varrho_1^{p-1}$. Irgend ein beliebige Periode aber ist $P_n = \varrho_n + \varrho_{n(p-1)} = \varrho_1^n + \varrho_1^{n(p-1)}$ oder auch $= \varrho_n + \varrho_{p-n} = \varrho_1^n + \varrho_1^{p-n}$. Da $\varrho_1^n = cos\,\frac{2n\pi}{p} + sin\,\frac{2n\pi}{p}\,.\,i$, $\varrho_1^{n(p-1)} = cos\,\frac{2n\pi}{p} - sin\,\frac{2n\pi}{p}\,.\,i$ ist; so hat man

$$P_n = 2\,cos\,\frac{2n\pi}{p} \tag{40}$$

Hieraus folgt, dass für $r = \frac{p-1}{2}$ alle Perioden P reelle Werthe haben, dass also die Gleichung r-ten Grades, deren Wurzeln die Werthe der verschiedenen P darstellen, lauter reelle Wurzeln hat. Jede beliebige dieser Wurzeln wie P_n liefert die Beziehungen

$$cos\,\frac{2n\pi}{p} = \frac{1}{2}P_n \qquad sin\,\frac{2n\pi}{p} = \sqrt{1-\frac{1}{4}P_n^2}$$

und demzufolge den Werth der Grösse ϱ_n mittelst der Formel

$$\varrho_n = \frac{1}{2}P_n + \sqrt{1-\frac{1}{4}P_n^2}\,\sqrt{-1} \tag{41}$$

Die Auflösung der fraglichen Gleichung vom Grade $r = \frac{p-1}{2}$ liefert also vermittelst ihrer Wurzeln P die vollständige Auflösung des Problems mit Hülfe der Formel (41). Denn jeder beliebige Werth von P führt zur Kenntniss einer Wurzel ϱ_n der Gleichung vom Grade $p-1$ und jede solche Wurzel ergiebt auch durch ihre Potenzen ϱ_n^1, ϱ_n^2, ϱ_n^3 ... ϱ_n^{p-1} diese sämmtlichen Wurzeln. Die Wurzel ϱ_1 ist diejenige von allen, deren reeller Theil der grösste positive und deren imaginärer Theil der kleinste positive ist.

5) Wenn $r = 2$, $s = \frac{p-1}{2}$ ist, wenn also zwei s-gliedrige Perioden P_1 und P_2 aus einer quadratischen Gleichung zu bestimmen sind; so kann jede Wurzel dieser Gleichung zu P_1 und die andere zu P_2 angenommen werden. Jeder Zweifel über die Reihenfolge der Grössen P ist hierdurch beseitigt.

6) Wenn $r = 3$, $s = \frac{p-1}{3}$ ist, wenn also drei s-gliedrige Perioden P_1, P_2, P_3 aus einer kubischen Gleichung zu bestimmen sind; so sind die ersten Glieder dieser Perioden die Potenzen der Einheitswurzel ϱ_1 von den Graden a^0, a^1, a^2, die zweiten Glieder sind die Potenzen von den Graden a^3, a^4, a^5 u. s. w., oder man hat

$$\begin{aligned} P_1 &= \varrho_1^{a^0} + \varrho_1^{a^3} + \varrho_1^{a^6} + \ldots \\ P_2 &= \varrho_1^{a^1} + \varrho_1^{a^4} + \varrho_1^{a^7} + \ldots \\ P_3 &= \varrho_1^{a^2} + \varrho_1^{a^5} + \varrho_1^{a^8} + \ldots \end{aligned}$$

Da 2 eine zu 3 relativ prime Zahl ist; so kann nach dem in Nr. 2 aufgestellten allgemeinen Satze $\alpha = 2$ genommen werden, d. h. es kann auch P_1, P_3, P_2 als eine zulässige Reihenfolge der Grössen P angesehen werden. Da nun jede beliebige der drei Grössen P_1, P_2, P_3 zur ersten angenommen werden kann; so erkennt man, dass auch jede beliebige der übrigen beiden zur zweiten gewählt werden kann, dass also jede beliebige Reihenfolge dieser drei Grössen eine zulässige ist. Um zu zeigen, wie aus einer ersten jede beliebige andere Reihenfolge theils durch Substitution einer anderen Potenz von ϱ_1 für ϱ, theils durch Wechsel der primitiven Wurzel a entsteht, bemerken wir Folgendes. Durch Substitution von $\varrho_n = \varrho_1^n$ für ϱ_1 ergiebt sich

$$\begin{aligned} P_{n_1} &= \varrho_1^{na^0} + \varrho_1^{na^3} + \varrho_1^{na^6} + \ldots \\ P_{n_2} &= \varrho_1^{na^1} + \varrho_1^{na^4} + \varrho_1^{na^7} + \ldots \\ P_{n_3} &= \varrho_1^{na^2} + \varrho_1^{na^5} + \varrho_1^{na^8} + \ldots \end{aligned}$$

oder, wenn $n \equiv a^\nu \bmod p$ ist,

$$\begin{aligned} P_{n_1} &= \varrho_1^{a^\nu} + \varrho_1^{a^{\nu+3}} + \varrho_1^{a^{\nu+6}} + \ldots \\ P_{n_2} &= \varrho_1^{a^{\nu+1}} + \varrho_1^{a^{\nu+4}} + \varrho_1^{a^{\nu+7}} + \ldots \\ P_{n_3} &= \varrho_1^{a^{\nu+2}} + \varrho_1^{a^{\nu+5}} + \varrho_1^{a^{\nu+8}} + \ldots \end{aligned}$$

Es leuchtet ein, dass die drei Perioden P_{n_1}, P_{n_2}, P_{n_3} den ersten drei Perioden P_1, P_2, P_3 gleich sind und dieselbe zyklische Reihenfolge bilden, wenn man P_1 oder P_2 oder P_3 voranstellt oder für P_{n_1} setzt, jenachdem ν den Werth $3t$ oder den Werth $3t+1$ oder den Werth $3t+2$ hat. Hieraus folgt, dass wenn erst einmal eine zulässige Reihenfolge der drei Wurzeln der fraglichen kubischen Gleichung gefunden ist, jede dieser Wurzeln in dieser Reihenfolge voran gestellt werden kann.

Wählen wir jetzt statt der primitiven Wurzel a eine andere b und ist $b \equiv a^\mu \bmod p$; so werden die drei Perioden zunächst

$$\begin{aligned} Q_1 &= \varrho_1^{b^0} + \varrho_1^{b^3} + \varrho_1^{b^6} + \ldots \\ Q_2 &= \varrho_1^{b^1} + \varrho_1^{b^4} + \varrho_1^{b^7} + \ldots \\ Q_3 &= \varrho_1^{b^2} + \varrho_1^{b^5} + \varrho_1^{b^8} + \ldots \end{aligned}$$

und wenn man a^μ für b setzt,

$$\begin{aligned} Q_1 &= \varrho_1^{a^0} + \varrho_1^{a^{3\mu}} + \varrho_1^{a^{6\mu}} + \ldots \\ Q_2 &= \varrho_1^{a^\mu} + \varrho_1^{a^{4\mu}} + \varrho_1^{a^{7\mu}} + \ldots \\ Q_3 &= \varrho_1^{a^{2\mu}} + \varrho_1^{a^{5\mu}} + \varrho_1^{a^{8\mu}} + \ldots \end{aligned}$$

Die erste dieser Perioden Q_1 ist gleich der früheren ersten Periode P_1, die zweite Q_2 ist jedoch nur dann gleich der früheren zweiten P_2, wenn $\mu = 3t+1$ ist, dagegen gleich der früheren dritten P_3, wenn

$\mu = 3t + 2$ ist. Da der letztere Fall nach dem Obigen so gut möglich ist, wie der erstere; so muss es, wenn $p - 1$ durch 3 theilbar ist, immer eine zweite primitive Wurzel b geben, welche einer Potenz a^μ kongruent ist, deren Exponent $\mu = 3t + 2$ ist, oder es muss Potenzen von a mit Exponenten von der Form $3t + 2$ geben, welche primitive Wurzeln darstellen oder ihnen äquivalent sind. Mit Hülfe einer solchen primitiven Wurzel kann $Q_2 = P_2$ werden, und da nach dem vorhergehenden Satze in der zyklischen Reihenfolge der Grössen P jede die erste sein kann; so ist auch die Reihenfolge P_1, P_3, P_2 mit jeder dieser drei Grössen als Anfangsgliede darstellbar. Aus allem Diesen folgt, dass die drei Wurzeln P der fraglichen kubischen Gleichung in jeder willkürlichen Reihenfolge für P_1, P_2, P_3 genommen werden können.

Durch dieses Resultat ist die in Kummer's Theorie, sowie in Bachmann's Lehre von der Kreistheilung offen gebliebene Frage, von welcher Letzterer ausdrücklich anerkennt, dass sie ihrer Lösung noch harre (15. Vorlesung Nr. 6, S. 217 und 218), zur Entscheidung gebracht. Übrigens hat sich Kummer nur um den Fall $r = 3$ bemüht, ohne auf die Untersuchung des allgemeinen Falles einzugehen, mit dem wir uns nachstehend ebenfalls befassen werden.

7) Angenommen, r sei irgend ein Faktor von $p - 1$, also $p = rs + 1$, und jede der r Perioden $P_1, P_2 \ldots P_r$ habe daher s Glieder, welche lauter Potenzen von ϱ_1 darstellen. Wenn die Werthe dieser r Grössen P als die Wurzeln einer Gleichung r-ten Grades dargestellt sind, entscheidet sich die Frage nach der zulässigen Reihenfolge derselben folgendermaassen. Nehmen wir irgend eine derselben für P_1 an, was nach dem Vorstehenden zulässig ist; so müssen die übrigen dem im vorigen Paragraphen entwickelten Gesetze gehorchen, es muss also zunächst

$$P_1^2 = 1_0\, s + 1_1\, P_1 + 1_2\, P_2 + \ldots + 1_r\, P_r \tag{42}$$

sein, worin die Koeffizienten $1_0, 1_1, 1_2 \ldots 1_r$ nach dem Obigen darstellbar sind. Wenn der hierzu im vorigen Paragraphen gewiesene Weg wegen der Auflösung unbestimmter Gleichungen höherer Grade zu beschwerlich wird, kann man das in §. 5 bezeichnete Verfahren in Anwendung bringen, indem man für a irgend eine primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \bmod p$ annimmt. Dasselbe ergiebt mit leichter Mühe die Grundtafel der Reste, worin die erste Reihe die Exponenten der Potenzen von ϱ_1 enthält, welche die Periode P_1 bilden. Eine Addition des ersten Restes 1 zu allen Resten dieser ersten Reihe führt zur Kenntniss der Koeffizienten der Gl. (42), indem jeder einzelne der sich ergebenden Reste anzeigt, dass diejenige Reihe P, welcher er angehört, voll in den Werth von P_1^2 tritt, während die sich etwa ergebenden Nullreste ebenso vielmal die Grösse $s\,\varrho^0 = s$ repräsentiren. Ebenso leicht erhält man aus der Grundtafel die Koeffizienten der Produkte

$$P_1 P_2 = 2_0 P_0 + 2_1 P_1 + 2_2 P_2 + \ldots$$
$$P_1 P_3 = 3_0 P_0 + 3_1 P_1 + 3_2 P_2 + \ldots$$

u. s. w.

Aus P_1^2 ergiebt sich durch Multiplikation mit P_1 die dritte Potenz von P_1 nach der Formel

$$P_1^3 = 1_0 s P_1 + 1_1 P_1^2 + 1_2 P_1 P_2 + 1_3 P_1 P_3 + \ldots + 1_r P_1 P_r$$

indem die Darstellung von $P_1 P_n$ nur die Addition von 1 zu den Resten der Reihe P_n erfordert. Setzt man für P_1^2, $P_1 P_2$, $P_1 P_3$ ... ihre linearen Werthe; so findet man für P_1^3 den linearen Ausdruck

$$(43) \qquad P_1^3 = 1_0' s + 1_1' P_1 + 1_2' P_2 + \ldots + 1_r' P_r$$

In ähnlicher Weise ergeben sich durch wiederholte Multiplikationen mit P_1 und Substitution der linearen Werthe der zweidimensionalen Produkte die aufsteigenden Potenzen von P_1 in der Form

$$(44) \qquad P_1^4 = 1_0'' s + 1_1'' P_1 + 1_2'' P_2 + \ldots + 1_r'' P_r,$$

u. s. f. bis

$$(45) \qquad P_1^r = \pi_0 s + \pi_1 P_1 + \pi_2 P_2 + \ldots + \pi_r P_r$$

Diese $r-1$ Gleichungen (42) bis (45) enthalten die $r-1$ Unbekannten $P_2, P_3 \ldots P_r$ und sind für alle vom ersten Grade, können also dafür aufgelöst werden. Hierdurch ergiebt sich jede der letzteren Grössen als eine bestimmte eindeutige Funktion von P_1, und es erscheinen danach die Grössen $P_1, P_2 \ldots P_r$ geordnet.

Die Auflösung der letzteren $r-1$ Gleichungen ergiebt zugleich eine bemerkenswerthe Beziehung zwischen den Wurzeln der Periodengleichung r-ten Grades, und man erkennt, dass man nur eine einzige dieser Wurzeln zu berechnen braucht, um daraus alle übrigen darzustellen.

Selbstredend liefert eine andere primitive Wurzel a der Kongruenz $x^{p-1} \equiv 1$ eine andere Grundtafel und damit eine andere Reihenfolge der P. Eine einzige Reihenfolge genügt aber, um daraus alle übrigen herzustellen. Denn es ist leicht zu übersehen, dass die in Nr. 2 gekennzeichnete Reihenfolge $P_1, P_{1+a}, P_{1+2a} \ldots$, wenn a eine zu r relativ prime Zahl ist, auch jetzt, wo P eine mehrgliedrige Reihe ist, Gültigkeit behält.

8) Zur Erläuterung des Vorstehenden an einem Beispiele hat man für $p = 31 = 2 \cdot 3 \cdot 5 + 1$, wenn man $r = 3$, $s = 10$ nimmt und die primitive Wurzel $a = 3$ zu Grunde legt, die Grundtafel der Reste

P_1	1	27	16	29	8	30	4	15	2	23
P_2	3	19	17	25	24	28	12	14	6	7
P_3	9	26	20	13	10	22	5	11	18	21

Die Koeffiziententafel ist

1	3	4	2
	4	2	4
	2	4	4

Man hat also

$$P_1^2 = 10 + 3 P_1 + 4 P_2 + 2 P_3$$
$$P_1^3 = 10 P_1 + 3 P_1 P_2 + 4 P_1 P_2 + 2 P_1 P_3$$
$$= 2 P_1 + 4 P_2 + 4 P_3$$

und aus diesen beiden Gleichungen folgt

$$32\,P_2 = -P_1^3 + 15\,P_1^2 - 6\,P_1 - 120$$
$$16\,P_3 = P_1^3 - 7\,P_1^2 - 18\,P_1 + 40$$

Hierdurch sind die Werthe von P_2 und P_3 bestimmt, wenn man für P_1 irgend eine der drei Wurzeln der kubischen Periodengleichung aus §. 6 Nr. 25 setzt.

Diese Periodengleichung muss sich offenbar herstellen, wenn man die letzte Gleichung mit 2 multiplizirt, alsdann zu der ersten addirt und beiderseits 32 P_1 hinzufügt. Da nämlich $P_1 + P_2 + P_3 = -1$ ist; so verschwinden die Grössen P_2 und P_3 und es bleibt eine kubische Gleichung für P_1 zurück, welche

$$P_1^3 + P_1^2 - 10\,P_1 - 8 = 0$$

ist und mit der erwähnten Periodengleichung genau übereinstimmt, wenn man darin $p = 31$ und $2_3 = 4$ setzt.

9) Das letzte Resultat ist von grosser Wichtigkeit, da es eine allgemeine Gültigkeit hat. Addirt man nämlich die aus den $r-1$ Gleichungen (43) bis (45) gefundenen Werthe von $P_2, P_3 \ldots P_r$ und dazu den Werth von P_1 und setzt die Summe $= -1$; so hat man sofort, indem man P_1 durch x ersetzt, die Periodengleichung r-ten Grades, welche die Grössen $P_1, P_2 \ldots P_r$ zu Wurzeln hat. Hieraus ergiebt sich, dass die Periodengleichung auf einem einfachen Wege dargestellt werden kann, ohne dass man nöthig hat, die symmetrischen Funktionen der P zu bilden. Man kann vielmehr, umgekehrt, diese symmetrischen Funktionen aus der gefundenen Gleichung ableiten, indem man die Koeffizienten von P_1^{r-1}, P_1^{r-2}, P_1^{r-3} etc. resp. gleich $-F(P_1)$, $+F(P_1P_2)$, $-F(P_1P_2P_3)$ etc. setzt.

Ausserdem leuchtet ein, dass man aus der Periodengleichung r-ten Grades nur eine einzige Wurzel zu berechnen braucht, indem man die übrigen $r-1$ Wurzeln leichter aus den linearen Gleichungen (43) bis (45) herstellen kann, zumal man diese Herstellung zum Zweck des Ordnens dieser Wurzeln doch ausführen muss.

10) Wenn r eine Primzahl ist, also alle Zahlen $1, 2, 3 \ldots r-1$ relativ prim zu r sind, kann in der Reihenfolge P_1, $P_{1+\alpha}$, $P_{1+2\alpha}$ etc. für α jeder Werth von 1 bis $r-1$ angenommen werden, die zweite Periode $P_{1+\alpha}$ kann also jeden der Werthe $P_2, P_3 \ldots P_{r-1}$ annehmen. Daraus folgt, dass für einen Primwerth von r nicht bloss in die erste, sondern auch in die zweite Stelle der fraglichen Reihe jede beliebige Wurzel der Periodengleichung r-ten Grades gestellt werden kann oder dass für P_1 und P_2 zwei beliebige dieser Wurzeln angenommen werden können.

11) Die vorstehenden Sätze reichen zur vollständigen Auflösung der Aufgabe aus, wenn $p - 1 = 2q$ und q eine ungerade Primzahl ist, indem dann für $r = q$ die zweigliedrigen Perioden $P_1, P_2 \ldots P_r$ erhalten werden, aus welchen sich nach Nr. 4 alle Werthe $\varrho_1, \varrho_2, \varrho_3 \ldots$ ergeben. Ist jedoch q eine zusammengesetzte Zahl; so liefert das Verfahren nach Nr. 7 für irgend einen Faktor r von $p - 1 = rs$ die s-gliedrigen Perioden $P_1, P_2 \ldots P_r$. Behuf Zerlegung jedes einzelnen

P in die Theilperioden Q sei $s = r's'$, es sei also jedes P in r' Gruppen folgendermaassen zu zerlegen

$$\begin{aligned}
P_1 &= Q_1 + Q_2 + \ldots + Q_{r'} \\
P_2 &= Q_{r'+1} + Q_{r'+2} + \ldots + Q_{2r'} \\
P_3 &= Q_{2r'+1} + Q_{2r'+2} + \ldots + Q_{3r'} \\
&\ldots\ldots\ldots\ldots \\
P_r &= Q_{(r-1)r'+1} + Q_{(r-1)r'+2} + \ldots + Q_{rr'}
\end{aligned}$$

Für jedes P ergeben sich die r' Theilgruppen Q durch das in §. 5 gelehrte Verfahren als die Wurzeln einer Gleichung r'-ten Grades; nur die Reihenfolge derselben ist noch festzustellen.

Die in aufeinander folgenden Gruppen P, Q, R etc. enthaltenen Potenzen von ϱ ergeben sich leicht, wenn man statt ihrer die Exponenten der Potenzen der primitiven Wurzel a, denen die Reste der Grundtafel kongruent sind, niederschreibt: es ergiebt sich dann, indem jede Gruppe in einer einzigen horizontalen Reihe dargestellt ist,

$$Y = 0 \quad 1 \quad 2 \quad 3 \quad \ldots \quad (p-1)$$

$$Y \left\{ \begin{array}{lcccccc}
P_1 & = & 0 & r & 2r & 3r & \ldots \\
P_2 & = & 1 & r+1 & 2r+1 & 3r+1 & \ldots \\
P_3 & = & 2 & r+2 & 2r+2 & 3r+2 & \ldots \\
 & \ldots & \ldots & \ldots & \ldots & \ldots & \\
P_r & = & r-1 & 2r-1 & 3r-2 & 4r-2 & \ldots
\end{array} \right.$$

$$P_1 \left\{ \begin{array}{lcccccc}
Q_1 & = & 0 & r'r & 2r'r & \ldots \\
Q_2 & = & r & (r'+1)r & (2r'+1)r & \ldots \\
 & \ldots & \ldots & \ldots & \ldots & \\
Q_{r'} & = & (r'-1)r & (2r'-1)r & (3r'-1)r & \ldots
\end{array} \right.$$

$$P_2 \left\{ \begin{array}{lcccccc}
Q_{r'+1} & = & 1 & r'r+1 & 2r'r+1 & \ldots \\
Q_{r'+2} & = & r+1 & (r'+1)r+1 & (2r'+1)r+1 & \ldots \\
 & \ldots & \ldots & \ldots & \ldots & \\
Q_{2r'} & = & (r'-1)r+1 & (2r'-1)r+1 & (3r'-1)r+1 & \ldots
\end{array} \right.$$

$$P_3 \left\{ \begin{array}{lcccccc}
Q_{2r'+1} & = & 2 & r'r+2 & 2r'r+2 & \ldots \\
Q_{2r'+2} & = & r+2 & (r'+1)r+2 & (2r'+1)r+2 & \ldots \\
 & \ldots & \ldots & \ldots & \ldots & \\
Q_{3r'} & = & (r'-1)r+2 & (2r'-1)r+2 & (3r'-1)r+2 & \ldots
\end{array} \right.$$

u. s. w.

Wenn man den Exponenten des ersten Gliedes irgend eines Q gleich $mr + n$ setzt, worin $m < r'$ und $n < r$; so gehört dieses Q der höheren Gruppe P_{n+1} an und ist das $Q_{nr'+m+1}$.

In ähnlicher Weise zerlegt sich dann jede Gruppe Q in die Theilgruppen R mit r'' Gliedern, wovon die ersten folgende sind.

$$Q_1 \begin{cases} R_1 = 0 & r''r'r & 2r''r'r \ldots \\ R_2 = r'r & (r''+1)r'r & (2r''+1)r'r \ldots \\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot \\ R_{r''} = (r''-1)r'r & (2r''-1)r'r & (3r''-1)r'r \ldots \end{cases}$$

$$Q_2 \begin{cases} R_{r''+1} = r & (r''r'+1)r & \ldots \\ R_{r''+2} = (r'+1)r & [(r''+1)r'+1]r & \ldots \\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot \\ R_{2r''} = [(r''-1)r'+1]r & [(2r''-1)r'+1]r & \ldots \end{cases}$$

u. s. w.

$$Q_{r'} \begin{cases} R_{(r'-1)r''+1} = (r'-1)r & [(r''+1)r'-1] & \ldots \\ R_{(r'-1)r''+2} = (2r'-1)r & [(r''+2)r'-1]r & \ldots \\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot \\ R_{r'r''} = (r''r'-1)r & (2r''r'-1)r & \ldots \end{cases}$$

$$Q_{r'+1} \begin{cases} R_{r'r''+1} = 1 & r''r'r+1 & \ldots \\ R_{r'r''+2} = r'r+1 & (r''+1)r'r+1 & \ldots \\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot \\ R_{(r'+1)r''} = (r''-1)r'r+1 & (2r''-1)r'r+1 & \ldots \end{cases}$$

$$Q_{r''+2} \begin{cases} R_{(r'+1)r''+1} = r+1 & (r''r'+1)r+1 & \ldots \\ R_{(r'+1)r''+2} = (r'+1)r+1 & [(r''+1)r'+1]r+1 & \ldots \\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot \\ R_{(r'+2)r''} = [(r''-1)r'+1]r+1 & [(2r''-1)r'+1]r+1 & \ldots \end{cases}$$

u. s. w.

Jedes Produkt aus irgend zwei der Grössen Q kann vermittelst der in §. 5 angegebenen Rechnung als ein linearer Ausdruck dieser Grössen in der Form

$$Q_m Q_n = k_0 + k_1 Q_1 + k_2 Q_2 + \ldots + k_{r'r''} Q_{r'r''}$$

dargestellt werden, worin mehrere der Koeffizienten k gleich null sein können und der erste k_0 oder das Nullglied diejenige ganze Zahl ist, welche anzeigt, wie oft der Nullrest in dem Produkt $Q_m Q_n$ vorkömmt. Hiernach können alle Potenzen irgend eines Q in derselben Form dargestellt werden. Bildet man also aus

$$Q_1^2 = b_0 + b_1 Q_1 + b_2 Q_2 + \ldots$$

durch wiederholte Multiplikation mit Q_1 und Substitution der linearen Ausdrücke für Q_1^2, $Q_1 Q_2$, $Q_1 Q_3$ etc. die Gleichungen

$$Q_1^3 = c_0 + c_1 Q_1 + c_2 Q_2 + \ldots$$
$$Q_1^4 = d_0 + d_1 Q_1 + d_2 Q_2 + \ldots$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$Q_1^{r'r''} = k_0 + k_1 Q_1 + k_2 Q_2 + \ldots$$

so hat man, da für Q_1 ein beliebiger der für $Q_1, Q_2 \ldots Q_{r'r''}$ gefundenen Werthe angenommen werden kann, $r'r'' - 1$ Gleichungen, aus welchen die

Grössen $Q_2, Q_3, \ldots Q_{rr'}$, welche nur auf erster Potenz darin vorkommen, bestimmt oder geordnet werden können. Diese Rechnung ersetzt zugleich die Auflösung der Periodengleichungen, welche sich aus den Gruppen $P_2, P_3 \ldots P_r$ ergeben, und macht überhaupt nur die Ermittlung einer einzigen Wurzel der aus einer Gruppe P_1 sich ergebenden Periodengleichung nothwendig.

Wenn man die vorangestellten r Gleichungen für $P_1, P_2 \ldots P_r$ mit berücksichtigt, braucht man nur bis zu der Potenz von Q_1 vom Grade $rr' - r = r(r'-1)$ hinaufzusteigen, um die erforderliche Anzahl von Gleichungen zu erhalten.

12) Durch vorstehendes Verfahren kann man aus den geordneten Gruppen P die geordneten Gruppen Q, sodann aus diesen die geordneten Gruppen R u. s. f. herstellen. Liessen sich auf irgend eine Weise die ersten Theilgruppen Q von allen P, also die Werthe von $Q_1, Q_{r'+1}, Q_{2r'+1} \ldots$ darstellen; so würde Diess die ganze Operation erleichtern, indem man alsdann nur für die Theilgruppen des ersten P die Potenzen

$$\begin{aligned} Q_1^2 &= b_0 + b_1 Q_1 + b_2 Q_2 + \ldots \\ Q_1^3 &= c_0 + c_1 Q_1 + c_2 Q_2 + \ldots \\ &\cdots\cdots\cdots\cdots \\ Q_1^{r'-1} &= l_0 + l_1 Q_1 + l_2 Q_2 + \ldots \end{aligned}$$

zu bilden brauchte, um hieraus für die folgenden Gruppen durch zyklische Verschiebung der Zeiger die Gleichungen

$$\begin{aligned} Q_{r'+1}^2 &= b_0 + b_1 Q_{r'+1} + b_2 Q_{r'+2} + \ldots \\ Q_{r'+1}^3 &= c_0 + c_1 Q_{r'+1} + c_2 Q_{r'+2} + \ldots \\ &\cdots\cdots\cdots \\ Q_{r'+1}^{r'-1} &= l_0 + l_1 Q_{r'+1} + l_2 Q_{r'+2} + \ldots \end{aligned}$$

ferner

$$\begin{aligned} Q_{2r'+1}^2 &= b_0 + b_1 Q_{2r'+1} + b_2 Q_{2r'+2} + \ldots \\ Q_{2r'+1}^3 &= c_0 + c_1 Q_{2r'+1} + c_2 Q_{2r'+2} + \ldots \\ &\cdots\cdots\cdots \\ Q_{2r'+1}^{r'-1} &= l_0 + l_1 Q_{2r'+1} + l_2 Q_{2r'+2} + \ldots \end{aligned}$$

u. s. w., welche dieselben Koeffizienten wie die ersten haben, niederzuschreiben. Diess würde $r(r'-2)$ und unter Hinzurechnung der r Gleichungen für $P_1, P_2 \ldots P_r$ die erforderlichen $r(r'-1)$ Gleichungen ergeben, welche, weil die Potenzen auf der linken Seite nur bis zum Grade $r'-1$ ansteigen, viel kleinere Koeffizienten in sich aufnehmen, als bei der zuvor beschriebenen Operation.

Die vorstehende Bedingung kann folgendermaassen erfüllt werden, wenn r und r' zwei relativ prime Zahlen sind. Wir haben erst Y in die r Gruppen P durch Auflösung einer Gleichung r-ten Grades zerlegt und diese Gruppen geordnet, darauf haben wir jedes P in r' Gruppen Q mittelst Auflösung von ebenso vielen Gleichungen r'-ten Grades zerlegt und beabsichtigen, die letzteren zu ordnen. Zerlegt man jetzt erst Y in r' Gruppen P' durch Auflösung einer Gleichung r'-ten Grades und ordnet

dieselben nach dem Verfahren in Nr. 8, zerlegt darauf jedes P' in r Gruppen durch Auflösung von ebenso vielen Gleichungen r-ten Grades; so ergeben sich ebenfalls in ungeordneter Folge die Gruppen Q'. Die rr' Gruppen Q' enthalten die rr' Gruppen Q, jedoch in einer anderen Reihenfolge, welche sich aus den obigen Werthen von Q ergiebt, wenn man darin r und r' vertauscht. Man hat nämlich

$$P_1' \begin{cases} Q_1' = 0 & rr' & 2rr' & \dots \\ Q_2' = r' & (r+1)r' & (2r+1)r' & \dots \\ Q_3' = 2r' & (r+2)r' & (2r+2)r' & \dots \\ \cdot \quad \cdot & \cdot \quad \cdot & \cdot \quad \cdot & \\ Q_r' = (r-1)r' & (2r-1)r' & (3r-1)r' & \dots \end{cases}$$

$$P_2' \begin{cases} Q_{r+1}' = 1 & rr'+1 & 2rr'+1 \\ Q_{r+2}' = r'+1 & (r+1)r'+1 & (2r+1)r'+1 \\ Q_{r+3}' = 2r'+1 & (r+2)r'+1 & (2r+2)r'+1 \\ \cdot \quad \cdot & \cdot \quad \cdot & \cdot \quad \cdot \\ Q_{2r}' = (r-1)r'+1 & (2r-1)r'+1 & (3r-1)r'+1 \end{cases}$$

u. s. w.

Wenn man den Exponenten des ersten Gliedes irgend eines Q' gleich $m'r' + n'$ setzt, worin $m' < r$ und $n' < r'$; so gehört dieses Q' der höheren Gruppe $P'_{n'+1}$ an und ist das $Q'_{n'r+m'+1}$.

Hiernach und weil r und r' relativ prim sind, enthält jedes beliebige P und jedes beliebige P' ein gemeinschaftliches Q und zwar nur ein einziges. Insbesondere ist

$$Q_1' = Q_1, \quad Q'_{r+1} = Q_{r'+1}, \quad Q'_{2r+1} = Q_{2r'+1}$$

u. s. w., d. h. dasjenige Q, welches dem P_1 und P_1' gemeinschaftlich angehört, ist das Q_1, dasjenige, welches dem P_2 und P_2' angehört, ist das $Q_{r'+1}$ oder auch das Q'_{r+1} u. s. f. Allgemein, ist dasjenige Q, welches dem P_x und dem P_y angehört, das $Q_{(x-1)r'+m+1} = Q'_{(y-1)r+m'+1}$, für welches die Gleichheit der Exponenten $mr + n$ und $m'r' + n'$, also die Gleichung $mr + x - 1 = m'r' + y - 1$ oder $mr - m'r' = y - x$ in kleinsten Zahlen für m und m' besteht. Die gemeinschaftlichen Q in den Gruppen P und P' liefern also nicht allein die gesuchten ersten Gruppen Q in den Zerlegungen der P, sondern auch alle übrigen Q in geordneter Stellung und hieraus geht hervor, dass die Darstellung der P' und Q' neben den P und Q, also die Zerlegung nach den Faktoren r' und r neben den Zerlegungen nach den Faktoren r und r' jede weitere Operation behuf Feststellung der Reihenfolge der Q überflüssig macht.

13) Wenn die beiden Zahlen r und r' ein gemeinschaftliches Maass t haben, ist das vorstehende Verfahren nicht anwendbar, weil alsdann jede zwei Gruppen P und P' nicht ein einziges Q, sondern deren t miteinander gemein haben und demnach keine Entscheidung über die Stellung derselben in den Gruppen P und P' erfolgt. Für $r = r'$ ist das gemeinschaftliche Maass sogar gleich r, d. h. je zwei Gruppen P und P' enthalten r gemeinschaftliche Q, was auch leicht zu übersehen war, da die Ver-

tauschung der beiden Faktoren r und r' gar keine neuen P' und Q' ergeben kann.

Wenn $p-1$ keine anderen Primfaktoren als 2 und 3 enthält, kann man die Gruppen Q immer ordnen, auch wenn der Faktor 2 oder der Faktor 3 mehrmals aufeinander folgt. Denn nach Nr. 5 und 6 ist alsdann die Reihenfolge der Wurzeln der betreffenden Periodengleichung gleichgültig: es kömmt also nur darauf an, dass bei der Zerlegung jedes P dieselbe Reihenfolge der Wurzeln Q beobachtet werde. Letzteres aber kann für quadratische und kubische Gleichungen immer geschehen, wenn man deren Wurzeln durch die allgemeinen Formeln darstellt, welche ich in §. 4 und 5 meiner Beiträge zu der Theorie der Gleichungen angegeben habe, indem man die Periodengleichungen, welche zur Zerlegungen der P dienen, sämmtlich in derselben Weise auflös't oder für die einzelnen Q in jedem P die gleichnamigen allgemeinen Wurzelwerthe annimmt (was bei quadratischen Gleichungen darauf hinaus läuft, für alle ersten Q die Wurzelgrösse mit demselben und für alle zweiten Q diese Grösse mit dem entgegengesetzten Zeichen zu nehmen). So kann z. B. die Gleichung $x^p = 1$ für $p = 17 = 2^4 + 1$, für $p = 19 = 2 \cdot 3^2 + 1$, für $p = 37 = 2^2 \cdot 3^2 + 1$, für $p = 73 = 2^3\, 3^2 + 1$, für $p = 163 = 2 \cdot 3^4 + 1$ ohne Weiteres durch sukzessive Zerlegungen in 2 und 3 Theile aufgelös't werden.

14) Wenn $p-1$ andere Primfaktoren als 2 und 3 enthält und auch dann, wenn ausser dem Faktor 2 der Faktor 3 darin vorkömmt und man die kubischen Periodengleichungen nicht nach Nr. 13 behandeln will, kann man stets das Verfahren aus Nr. 12 in Anwendung bringen, wenn man Folgendes beachtet. Angenommen, $p-1$ sei in seine Primfaktoren $2, r, r', r'' \ldots$ aufgelös't und man habe $p - 1 = 2^\alpha r^\beta (r')^\gamma (r'')^\delta \ldots$ Lässt sich dieses Produkt in eine Folge von Primfaktoren zerlegen, in welcher je zwei benachbarte Faktoren ungleich sind; so kann man nach dieser Folge die Zerlegungen ausführen. So kann man z. B. für $p = 19$ $p - 1 = 3 \cdot 2 \cdot 3$, für $p = 37$ $p - 1 = 2 \cdot 3 \cdot 2 \cdot 3$, für $p = 73$ $p - 1 = 2 \cdot 3 \cdot 2 \cdot 3 \cdot 2$ nehmen.

Ist eine solche Reihenfolge nicht möglich, wie z. B. bei $p = 163 = 2 \cdot 3^4 + 1$; so beachte man, dass wie man in Nr. 12 von dem geordneten Y und den geordneten P zu den Q überging, indem man die beiden Faktoren r und r' vertauschte, also neben den P und Q auch die P' und Q' darstellte, man für einen folgenden Faktor r'' von den geordneten P und den geordneten Q zu den R übergehen kann, indem man die beiden Faktoren r' und r'' vertauscht, also neben den Q und R auch die Q'' und R'' darstellt. Immer kann man also, wenn eine Zerlegung in die r Grössen P, gleichviel, auf welchem Wege diese P gewonnen sind, ob durch einmalige oder durch mehrmalige Zerlegung, nachdem man daraus mittelst des Faktors r' die Q und dann mittelst des Faktors r'' die R hergestellt hat, durch die in Nr. 12 nachgewiesenen Beziehungen die Q'' und R'' herstellen, welche einer Vertauschung der Faktoren r' und r'' entsprechen, d. h. man kann aus den der Faktorenfolge $r\,r'\,r''$ entsprechenden Grössen P, Q, R die der Faktorenfolge $r\,r''\,r'$ entsprechenden Grössen P, Q'', R'' in geordneter Folge darstellen.

Hierdurch kann man offenbar bewirken, dass jeder beliebige in $p-1$ enthaltene Primfaktor wie r' nach jedem Zerlegungsakte der letzte wird und dass sich demselben dann ein ihm ungleicher Primfaktor anschliesst, sodass das Verfahren aus Nr. 12 immer aufs neue angewandt werden kann, bis alle Faktoren von $p-1$ erschöpft sind. So kann man in dem Beispiele $p = 163$ mit der Zerlegung $3 \cdot 2 \cdot 3$ beginnen, darauf durch Vertauschung der letzten beiden Faktoren die Zerlegung $3 \cdot 3 \cdot 2$ darstellen und hierauf $3 \cdot 3 \cdot 2 \cdot 3$ bilden. Vertauscht man jetzt wieder die beiden letzten Faktoren; so ergiebt sich die Zerlegung $3 \cdot 3 \cdot 3 \cdot 2$ und alsdann die $3 \cdot 3 \cdot 3 \cdot 2 \cdot 3$, welche den Schluss bildet.

Da $p-1$ den Faktor 2 enthält, der Fall aber, wo $p-1 = 2^\alpha$ ist, durch die Auflösung von quadratischen Gleichungen nach der obigen Vorschrift zu behandeln ist; so lässt sich jeder andere Fall, wo neben dem Faktor 2 noch ein anderer Primfaktor in $p-1$ enthalten ist, nach der vorstehenden Regel erledigen.

Um die Rechnung an einem einfachen Beispiele zu erläutern, sei für $p = 19 = 2 \cdot 3^2 + 1$ die Zerlegung nach den Faktoren $2 \cdot 3$ gebildet: man erhält hierfür, da 2 eine primitive Wurzel der Kongruenz $x^{18} \equiv 1 \pmod{19}$ ist,

$$Y = 1\ 2\ 4\ 8\ 16\ 13\ 7\ 14\ 9\ 18\ 17\ 15\ 11\ 3\ 6\ 12\ 5\ 10$$

$$Y_1 \begin{cases} P_1 = 1 & 4 & 16 & 7 & 9 & 17 & 11 & 6 & 5 \\ P_2 = 2 & 8 & 13 & 14 & 18 & 15 & 3 & 12 & 10 \end{cases}$$

$$P_1 \begin{cases} Q_1 = 1 & 7 & 11 \\ Q_2 = 4 & 9 & 6 \\ Q_3 = 16 & 17 & 5 \end{cases}$$

$$P_2 \begin{cases} Q_4 = 2 & 14 & 3 \\ Q_5 = 8 & 18 & 12 \\ Q_6 = 13 & 15 & 10 \end{cases}$$

Durch Vertauschung der Faktoren 2 und 3 ergiebt sich

$$Y \begin{cases} P_1' = 1 & 8 & 7 & 18 & 11 & 12 \\ P_2' = 2 & 16 & 14 & 17 & 3 & 5 \\ P_3' = 4 & 13 & 9 & 15 & 6 & 10 \end{cases}$$

$$P_1' \begin{cases} Q_1' = 1 & 7 & 11 = Q_1 \\ Q_2' = 8 & 18 & 12 = Q_5 \end{cases}$$

$$P_2' \begin{cases} Q_3' = 2 & 14 & 3 = Q_4 \\ Q_4' = 16 & 17 & 5 = Q_3 \end{cases}$$

$$P_3' \begin{cases} Q_5' = 4 & 9 & 6 = Q_2 \\ Q_6' = 13 & 15 & 10 = Q_6 \end{cases}$$

worin man die Q' aus den Q direkt durch die am Schlusse von Nr. 12 aufgestellten Relationen darstellen kann. Lässt man auf diese Zerlegung 3 . 2 den Faktor 3 folgen; so kömmt

$$Q_1' \begin{cases} R_1 = 1 \\ R_2 = 7 \\ R_3 = 11 \end{cases} \qquad Q_2' \begin{cases} R_4 = 8 \\ R_5 = 18 \\ R_6 = 12 \end{cases}$$

$$Q_3' \begin{cases} R_7 = 2 \\ R_8 = 14 \\ R_9 = 3 \end{cases} \qquad Q_4' \begin{cases} R_{10} = 16 \\ R_{11} = 17 \\ R_{12} = 5 \end{cases}$$

$$Q_5' \begin{cases} R_{13} = 4 \\ R_{14} = 9 \\ R_{15} = 6 \end{cases} \qquad Q_6' \begin{cases} R_{16} = 13 \\ R_{17} = 15 \\ R_{18} = 10 \end{cases}$$

Wollte man jetzt nochmals die beiden letzten Faktoren in der Reihenfolge 3 . 2 . 3 vertauschen, also die Zerlegung nach der Reihenfolge 3 . 3 . 2 darstellen; so erhielte man aus P_1', P_2', P_3'

$$P_1' \begin{cases} Q_1'' = 1\ 18 \\ Q_2'' = 8\ 11 \\ Q_3'' = 7\ 12 \end{cases} \qquad P_2' \begin{cases} Q_4'' = 2\ 17 \\ Q_5'' = 16\ 3 \\ Q_6'' = 14\ 5 \end{cases} \qquad P_3' \begin{cases} Q_7'' = 4\ 15 \\ Q_8'' = 13\ 6 \\ Q_9'' = 9\ 10 \end{cases}$$

und dann durch Zerlegung der Q''

$$Q_1'' \begin{cases} R_1'' = 1 \\ R_2'' = 18 \end{cases} \qquad Q_2'' \begin{cases} R_3'' = 8 \\ R_4'' = 11 \end{cases} \qquad Q_3'' \begin{cases} R_5'' = 7 \\ R_6'' = 12 \end{cases}$$

$$Q_4'' \begin{cases} R_7'' = 2 \\ R_8'' = 17 \end{cases} \qquad Q_5'' \begin{cases} R_9'' = 16 \\ R_{10}'' = 3 \end{cases} \qquad Q_6'' \begin{cases} R_{11}'' = 14 \\ R_{12}'' = 5 \end{cases}$$

$$Q_7'' \begin{cases} R_{13}'' = 4 \\ R_{14}'' = 15 \end{cases} \qquad Q_8'' \begin{cases} R_{15}'' = 13 \\ R_{16}'' = 6 \end{cases} \qquad Q_9'' \begin{cases} R_{17}'' = 9 \\ R_{18}'' = 10 \end{cases}$$

Erst die in Nr. 11 bis 14 vorgetragenen Sätze ermöglichen die Auflösung der Gleichung $x^p - 1 = 0$. Ohne diese Sätze konnte nach den bisher bekannten Regeln wohl der spezielle Fall, wo $p - 1 = 2^\alpha$ ist, durch quadratische Gleichungen (unter Beachtung der in Nr. 13 erwähnten Regel), aber kein Fall, wo in $p - 1$ ein anderer Primfaktor als 2 vorkömmt, gelös't werden.

§. 8. Die geometrische Bedeutung der Perioden.

Wenn durch Auflösung der Gleichung $x^p - 1 = 0$ irgend ein Werth von x gefunden ist; so stellt dieselbe irgend eine der p Wurzeln der Einheit vom Grade p dar. Ohne die Stellung dieser Wurzel ϱ in der

Reihe der Werthe von ϱ_n aus Gl. (39) zu kennen, ist dieselbe sofort geeignet, ein regelmässiges p-eck zu konstruiren, vorausgesetzt, dass nicht gerade $\varrho = 1$ sei, was übrigens, wenn ϱ durch die obigen Methoden aus der Gl. (38) gefunden worden, unmöglich ist: denn ϱ stellt immer irgend eine der $p-1$ gegen die Grundaxe geneigten Seiten dieses Polygons dar, und da p eine Primzahl ist; so liefern die sukzessiven Potenzen von ϱ, nämlich $\varrho^1, \varrho^2, \varrho^3, \ldots \varrho^p$ stets ein regelmässiges p-eck. Wählt oder trifft man in diesem ϱ die komplexe Wurzel ϱ_1 mit dem kleinsten Neigungswinkel; so werden diese Potenzen gleich den Seiten $\varrho_1, \varrho_2, \varrho_3 \ldots$ des gewöhnlichen p-ecks $A_0\ A_1\ A_2 \ldots$ (Fig. 9), worin die Seiten mit den Zeigern 1, 2, 3 ... bezeichnet sind. Wählt oder trifft man in dem gedachten ϱ eine andere, ausser der vorletzten Wurzel ϱ^{p-1}, also die Wurzel ϱ_1^n; so ergeben die Potenzen $\varrho_1^n, \varrho_1^{2n}, \varrho_1^{3n} \ldots \varrho_1^{pn}$ die Seiten $\varrho_n, \varrho_{2n}, \varrho_{3n} \ldots \varrho_{pn}$ eines sternförmigen p-ecks (Fig. 10), welches in den Durchschnittspunkten seiner Seiten, sowie in seinen Eckpunkten immer ein gewöhnliches p-eck darstellt. Für $\varrho = \varrho_1^{p-1} = \varrho_{p-1}$ entsteht das unter der Grundaxe liegende gewöhnliche p-eck (Fig. 11) und für $\varrho = \varrho_1^{p-n} = \varrho_{p-n}$ das unter dieser Axe liegende sternförmige p-eck, welches sich oberhalb dieser Axe für $\varrho = \varrho_1^n$ ergab.

Sind alle Wurzeln der Gleichung $x^p - 1 = 0$ in der Form $b + ci$ bekannt; so ist ihre Anordnung in der natürlichen Reihenfolge $\varrho_1, \varrho_2, \varrho_3 \ldots$ leicht, indem ϱ_1 diejenige Wurzel ist, welche das grösste positiv reelle Glied b und das kleinste positiv imaginäre Glied ci hat, während sich hieran als ϱ_2 die Wurzel mit nächst kleinerem positiv reellem und nächst grösserem positiv imaginärem Gliede anreihet, bis endlich die Wurzeln mit wachsendem negativ reellem und abnehmendem positiv imaginärem, dann die Wurzeln mit abnehmendem negativ reellem und wachsendem negativ imaginärem Gliede und zuletzt die Wurzeln mit wachsendem positiv reellem und abnehmendem negativ imaginärem Gliede folgen.

Stellt man für $r = \frac{1}{2}(p-1)$ die zweigliedrigen Perioden P_1, P_2, P_3 ... dar; so weiss man aus §. 7 Nr. 4, dass jede dieser Perioden wie $P_n = \varrho_n + \varrho_{p-n}$ die algebraische Summe zweier Seiten wie $A_1\ A_2$ und $A_4\ A_5$ (Fig. 12), welche gleich weit rechts und links von der Mittellinie $C\ A_3$ liegen, darstellt. Macht man also $A_1\ B_1$ parallel zu $A_5\ A_6$, ferner $A_2\ B_2$ parallel zu $A_4\ A_5$ u. s. f.; so stellen die Perioden P in irgend einer Reihenfolge die reellen Linien $A_0\ B_1$, $A_1\ B_2$, $A_2\ A_4$ etc. dar. Dieselben ordnen sich in der Weise, dass $\varrho_1 + \varrho_{p-1}$ den grössten positiven und $\varrho_2 + \varrho_{p-2}$ den nächst kleineren Werth besitzt, welcher endlich negativ wird, sodass das letzte $\varrho_r + \varrho_{p-r}$, welches die Diagonale $A_2\ A_4$ darstellt, den grössten negativen Werth hat. Jedes dieser P kann zur Konstruktion einer Seite des p-eckes dienen, indem man über demselben ein gleichschenkliges Dreieck wie z. B. $A_1\ B_2\ A_2$ beschreibt, dessen beide gleichen Seiten $A_1\ A_2$ und $B_2\ A_2$ gleich der Längeneinheit sind.

Zieht man die zur Grundaxe oder zur letzten Seite $A_6\ A_0$ parallelen Diagonalen $A_0\ A_6$, $A_1\ A_5$, $A_2\ A_4$ etc.; so stellen die Grössen P_1, P_2, P_3 ... die Differenzen dieser Diagonalen dar.

Beispielsweise sind für $p = 7$, $r = 3 = \frac{1}{2} \cdot 6$ die drei zweigliedrigen Perioden $P_1 = \varrho_1 + \varrho_6 = A_0 B_1$, $P_2 = \varrho_5 + \varrho_2 = A_1 B_1$, $P_3 = \varrho_4 + \varrho_3 = A_2 A_4$ und man hat

$$P_1 + P_2 + P_3 = A_0 B_1 + A_1 B_2 + A_2 A_4 = A_0 A_6 = -1$$

Die r Perioden $P_1, P_2 \ldots P_r$ von je $\frac{1}{r}(p-1)$ Gliedern, auf welchem Wege sie auch gewonnen sein mögen, können, wenn man allgemein den Rest von a^n mit a_n bezeichnet, stets in folgender Weise geordnet werden (wobei die mit den früheren Zeigern bezeichneten P nicht mehr dieselben sind).

$$\begin{aligned}
P_1 &= \varrho^{a^0} + \varrho^{a^r} + \varrho^{a^{2r}} + \ldots = \varrho^{a_0} + \varrho^{a_r} + \varrho^{a_{2r}} + \ldots \\
P_2 &= \varrho^{a^1} + \varrho^{a^{r+1}} + \varrho^{a^{2r+1}} + \ldots = \varrho^{a_1} + \varrho^{a_{r+1}} + \varrho^{a_{2r+1}} + \ldots \\
P_3 &= \varrho^{a^2} + \varrho^{a^{r+2}} + \varrho^{a^{2r+2}} + \ldots = \varrho^{a_2} + \varrho^{a_{r+2}} + \varrho^{a_{2r+2}} + \ldots \\
&\quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad ,
\end{aligned}$$

Diese Perioden sind also die algebraischen Summen von Einheitswurzeln oder, bei geometrischer Darstellung, von Linien $A_0 B_1$, $B_1 B_2$, $B_2 B_3$ etc. (Fig. 13), welche sämmtlich die Länge der Längeneinheit haben und deren Neigungswinkel $D A_0 B_1$, $D D_1 B_2$, $D D_2 B$ etc. gegen die Grundaxe $A_0 D$ die Glieder einer geometrischen Progression mit dem Exponenten a^r bilden. Bezeichnet φ den kleinsten Anfangswinkel $D A_0 B_1$ der ersten Periode P_1, also den Winkel $\sqrt[p]{2\pi}$, welcher dem ersten Gliede von P_1 zukömmt; so haben die Glieder von P_1 die Winkel φ, $a^r \varphi$, $a^{2r} \varphi \ldots$ oder wenn man die in diesen Winkeln enthaltenen ganzen Vielfachen von 2π abstreicht, die Winkel φ, $a_r \varphi$, $a_{2r} \varphi \ldots$ Setzt man diese Winkel resp. gleich ψ_0, ψ_1, $\psi_2 \ldots$; so sind die Winkel

von P_1 $\varphi, a^r\varphi, a^{2r}\varphi \ldots = \varphi, a_r\varphi, a_{2r}\varphi \ldots = \psi_0, \psi_1, \psi_2 \ldots$
„ P_2 $a\varphi, a^{r+1}\varphi, a^{2r+1}\varphi \ldots = a_1\varphi, a_{r+1}\varphi, a_{2r+1}\varphi \ldots = a\psi_0, a\psi_1, a\psi_2 \ldots$
„ P_3 $a^2\varphi, a^{r+2}\varphi, a^{2r+2}\varphi \ldots = a_2\varphi, a_{r+2}\varphi, a_{2r+2}\varphi \ldots = a^2\psi_0, a^2\psi_1, a^2\psi_2 \ldots$

u. s. w. Durch die r Perioden P werden also die p Seiten des regelmässigen p-eckes vermittelst eines im Allgemeinen unregelmässigen $(r+1)$-eckes $A_0 B_3 E$ dargestellt, dessen eine Seite $A_0 E = -1$ ist, während die übrigen r Seiten $A_0 B_3$ und $B_3 E$, welche den über der Seite $A_0 E$ stehenden $(p-1)$-gliedrigen Theil des p-eckes ersetzen, die Werthe der Perioden $P_1, P_2 \ldots P_r$ haben und jede dieser Perioden sich als ein Polygon von $\frac{1}{r}(p-1)$ Seiten darstellt, deren Längen gleich 1 sind und deren Neigungswinkel die bezeichnete geometrische Progression befolgen und durch die in dem betreffenden P enthaltenen Reste der Grundtafel, wenn dieselben mit φ multiplizirt werden, ersetzt werden können. So sind z. B. für $p = 7$, $r = 2$, $a = 3$ die Winkel

der Glieder der beiden dreigliedrigen Perioden $P_1 = A_0\ B_3$ und $P_2 = A_0\ C_3 = B_3\ E$

$$\text{in } P_1 = A_0\ B_3 \qquad 3^0\varphi,\ 3^2\varphi,\ 3^4\varphi = 1\varphi,\ 2\varphi,\ 4\varphi$$
$$\text{in } P_2 = A_0\ C_3 \qquad 3^1\varphi,\ 3^3\varphi,\ 3^5\varphi = 3\varphi,\ 6\varphi,\ 5\varphi$$

Da in diesem Beispiele $P_1 = \varrho_1 + \varrho_2 + \varrho_4$ und $P_2 = \varrho_3 + \varrho_6 + \varrho_5$ ist; so hat man auch $P_1 - P_2 = (\varrho_1 - \varrho_6) + (\varrho_2 - \varrho_5) - (\varrho_3 - \varrho_4)$. In dem regelmässigen Siebeneck (Fig. 12) ist der Abstand der Diagonalen $A_0\ A_6$ und $A_1\ A_5$ gleich $\frac{1}{2}(\varrho_1 - \varrho_6)$, der Abstand der Diagonalen $A_1\ A_5$ und $A_2\ A_4$ gleich $\frac{1}{2}(\varrho_2 - \varrho_5)$ und der Abstand der Diagonalen $A_2\ A_4$ von A_3 gleich $\frac{1}{2}(\varrho_3 - \varrho_4)$. Da man nun $P_1 + P_2 = -1$, $P_1\ P_2 = 2$ und demnach die Periodengleichung $x^2 + x + 2 = 0$ hat, woraus sich $P_1 = -\frac{1}{2} + \frac{1}{2}\sqrt{-7}$, $P_2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-7}$, also $P_1 - P_2 = \sqrt{-7}$ findet; so ist in dem Siebeneck die Differenz zwischen den Abständen CD und DA_3 gleich $\frac{1}{2}\sqrt{-7}$ oder die absolute Länge dieser Differenz gleich $\frac{1}{2}\sqrt{7}$. Hat CF diese Länge; so ist $A_0\ F = P_1$ und in der That ist $A_2\ F$ gleich und parallel $A_3\ A_4$, folglich algebraisch $A_0\ F = (A_0\ A_1) + (A_1\ A_2) + (A_3\ A_4) = \varrho_1 + \varrho_2 + \varrho_4$.

§. 9. Die Fälle, wo p keine Primzahl ist.

1) Wenn p keine Primzahl ist, aber mehrere verschiedene Primfaktoren hat; so lässt sich p in mehrere relativ prime Faktoren zerlegen. Ist $p = rs$ und r und s relativ prim; so ist die Auflösung der Gleichung $x^p - 1 = 0$ gesichert, wenn man die beiden Gleichungen $x^r - 1 = 0$ und $x^s - 1 = 0$ auflösen kann. Denn ist ϱ irgend eine von 1 verschiedene Wurzel der ersten und σ eine solche der zweiten Gleichung; so ist die Differenz $\varrho - \sigma$ dieser beiden Wurzeln immer einer Diagonalen in dem regelmässigen p-eck also auch einer Seite desselben und zwar einer nicht in dem r-eck und nicht dem s-eck liegenden Seite parallel. Setzt man daher

$$\varrho - s = a + bi = \sqrt{a^2 + b^2}\left(\frac{a}{\sqrt{a^2 + b^2}} + \frac{a}{\sqrt{a^2 + b^2}}\,i\right)$$

so ist $\frac{a}{\sqrt{a^2 + b^2}} + \frac{b}{\sqrt{a^2 + b^2}} \cdot i$ die fragliche der Diagonalen parallele Seite des p-eckes. (Die Richtigkeit dieses Satzes erhellet sofort, wenn

man in dem regelmässigen p-eck alle Radien zieht. Dieselben sind den Seiten des Polygons parallel, und die Differenz irgend zweier Radien, wie $OA - OB = -(AO + OB) = -AB = BA$ in Fig. 14 ist einer Polygonseite CD parallel). Die sukzessiven Potenzen der eben gedachten Seite ergeben, weil r und s relativ prim sind, alle p Seiten des p-eckes, also alle Auflösungen der Gleichung $x^p - 1 = 0$.

Ist p das Produkt $r\,s\,t\,\ldots$ mehrerer Faktoren $r, s, t\,\ldots$, wovon je zwei relativ prim sind, und ist $\varrho, \sigma, \tau\,\ldots$ je eine Wurzel der Gleichung $x^r - 1 = 0$, $x^s - 1 = 0$, $x^t - 1 = 0$ u. s. w.; so liefert die Differenz $\varrho - \sigma$ nach Vorstehendem eine Seite des $(r\,s)$-eckes oder eine Wurzel ϱ' der Gleichung $x^{rs} - 1 = 0$. Ferner liefert die Differenz $\varrho' - \tau$ in derselben Weise eine Seite des $(r\,s\,t)$-eckes oder eine Wurzel der Gleichung $x^{rst} - 1 = 0$. Auf diese Weise wird die Gleichung $x^p - 1$ auf Gleichungen derjenigen niedrigeren Grade $r, s, t\,\ldots$ zurückgeführt, welche die kleinsten relativ primen Faktoren von p darstellen.

Sind $r, s, t\,\ldots$ verschiedene Primzahlen und $p = r^\alpha s^\beta t^\gamma\,\ldots$; so kann auf diese Weise die Gleichung auf Gleichungen von den Graden r^α, s^β, $t^\gamma\,\ldots$, jedoch nicht von niedrigeren Graden zurückgeführt werden: sind also alle Exponenten $\alpha, \beta, \gamma\,\ldots$ gleich 1; so geschieht die Auflösung durch die Auflösung der Gleichungen $x^r - 1 = 0$, $x^s - 1 = 0$, $x^t - 1 = 0$ etc. nach der früheren Methode: ist aber einer dieser Exponenten > 1; so kömmt es darauf an, die Gleichung $x^p - 1 = 0$ für den Fall aufzulösen, dass p die Potenz r^α einer Primzahl ist.

Das einfachste Verfahren ist natürlich die Auflösung der Gleichung $x^r - 1 = 0$ nach der früheren Methode, und wenn ϱ irgend eine Wurzel derselben ist, die wiederholte Ausziehung der r-ten Wurzel aus ϱ. Handelt es sich z. B. um die Gleichung $x^9 - 1 = 0$ oder um die Darstellung des regelmässigen Neuneckes; so ist die Gleichung $x^3 - 1 = 0$, weil die Primzahl $3 = 2 + 1$ ist, durch quadratische Gleichungen auflösbar. (was natürlich nicht von der Gleichung $x^9 - 1 = 0$ gesagt werden kann). Da man für die Wurzeln der Gleichung $x^3 - 1 = 0$ ausser der Wurzel $x = 1$ die beiden Wurzeln $x = -\frac{1}{2} \mp \frac{1}{2}\sqrt{-3}$ erhält; so sind die 9 Wurzeln der Gleichung neunten Grades durch $x = \sqrt[3]{1}$ und $x = \sqrt[3]{-\frac{1}{2} \mp \sqrt{-3}}$ dargestellt.

2) Durch die vorstehenden oder ähnliche Sätze kann jede Gleichung $x^p - 1 = 0$ leicht auf die einfachsten Formen zurückgeführt werden: es ist jedoch wegen der dabei zu Tage tretenden Zahlengesetze nützlich zu zeigen, wie auch die früheren Prinzipien der Kreistheilung auf den allgemeinen Fall eines zusammengesetzten p Anwendung finden.

Zunächst ist klar, dass wenn r irgend ein Faktor von $p = r\,s$ ist, die Seiten ϱ_r, $\varrho_{2r}\,\ldots\,\varrho_p$ oder auch, wenn man $\varrho_{sr} = \varrho^{sr} = 1$ mit $\varrho_0 = \varrho^0 = 1$ vertauscht, die Seiten ϱ_0, ϱ_r, $\varrho_{2r}\,\ldots\,\varrho_{(s-1)r}$ des p-eckes ein regelmässiges r-eck bilden, dass man also für jeden Faktor von p

(46) $$\varrho_r + \varrho_{2r} + \ldots + \varrho_p = \varrho^r + \varrho^{2r} + \ldots + \varrho^p = 0$$

und wenn man $\varrho^r = \sigma$ setzt,

$$\sigma^1 + \sigma^2 + \ldots + \sigma^s = 0 \quad \text{oder}$$

(47) $$\sigma^{s-1} + \sigma^{s-2} + \ldots + \sigma = -1$$

hat. Ist s eine Primzahl; so kann die letzte Gleichung ganz nach der früheren bei Auflösung der Gleichung $x^s - 1 = 0$ angewandten Methode behandelt, folglich der Werth jeder der Grössen $\sigma, \sigma^2, \ldots \sigma^{s-1}$ festgestellt werden. Hat man auf diese Weise σ für jeden Primfaktor s von p gefunden; so ergiebt sich auch das σ für jeden zusammengesetzten Faktor rs von p durch die Formel $\sqrt[r]{\sigma}$.

Sind $r, s, t \ldots$ überhaupt n verschiedene Primzahlen und $p = rst \ldots$; so sind in den Gliedern der n Gleichungen

(48)
$$\begin{cases} \varrho^r + \varrho^{2r} + \ldots + \varrho^p = 0 \\ \varrho^s + \varrho^{2s} + \ldots + \varrho^p = 0 \\ \varrho^t + \varrho^{2t} + \ldots + \varrho^p = 0 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{cases}$$

sämmtliche Potenzen von ϱ enthalten, deren Exponenten ein gemeinschaftliches Maass mit p besitzen: manche dieser Potenzen kommen jedoch mehrmals unter diesen Gliedern vor. Addirt man alle diese Gleichungen; so hat man auf der rechten Seite den Nullwerth, auf der linken Seite aber bleiben die Potenzen, deren Exponenten ein gemeinschaftliches Maass mit p haben, und zwar eine jede nur ein einziges Mal zurück, wenn man folgendermaassen verfährt. Man subtrahirt den Komplex von Gliedern, welche je zwei jener Gleichungen miteinander gemein haben, also die Komplexe

$$\begin{array}{l} \varrho^{rs} + \varrho^{2rs} + \ldots + \varrho^p = 0 \\ \varrho^{rt} + \varrho^{2rt} + \ldots + \varrho^p = 0 \\ \varrho^{st} + \varrho^{2st} + \ldots + \varrho^p = 0 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{array}$$

Darauf addirt man die Komplexe, welche je drei jener Gleichungen miteinander gemein haben, also die Komplexe

$$\varrho^{rst} + \varrho^{2rst} + \ldots + \varrho^p = 0$$

Alsdann subtrahirt man die Komplexe, welche je vier jener Gleichungen miteinander gemein haben. Schliesslich ist der Komplex, welchen alle n Gleichungen miteinander gemein haben, zu subtrahiren, wenn n paar ist, und zu addiren, wenn n unpaar ist. Während nun alle vorher subtrahirten und addirten Komplexe $= 0$ sind, besteht der letzte Komplex aus der einzigen Grösse $\varrho^p = 1$. Bezeichnet man also die Summe aller p Potenzen $\varrho^1 + \varrho^2 + \ldots + \varrho^p$ mit A, die Summe aller derjenigen Potenzen, deren Exponenten ein gemeinschaftliches Maass mit p haben (mit Ausschluss der Potenz ϱ vom Exponenten 1, aber mit Einschluss der Potenz $\varrho^p = \varrho^0 = 1$), mit B und die Summe aller derjenigen Potenzen, deren Exponenten relativ prim zu p sind (mit Ausschluss der Potenz $\varrho^p = \varrho^0 = 1$, aber mit Einschluss der Potenz ϱ vom Ex-

ponenten 1) mit Y; so ist immer $A = 0$, B aber hat in dem eben erörterten Falle, wo $p = r\,s\,t\,\ldots$ aus n verschiedenen Primfaktoren besteht, den Werth

$$B = (-1)^{n+1} \tag{49}$$

und demzufolge ist $A - B$ oder

$$Y = (-1)^n \tag{50}$$

Wenn p irgend einen Primfaktor auf einer höheren als der ersten Potenz enthält, wenn also $p = r^\alpha\, s^\beta\, t^\gamma \ldots$ ist und unter den Exponenten $\alpha, \beta, \gamma \ldots$ mindestens einer > 1 ist; so enthalten die Gleichungen (48) alle Potenzen, deren Exponenten ein gemeinschaftliches Maass mit p haben, und die Ausscheidung der mehrfach vorkommenden gleichen Potenzen geht in derselben Weise vor sich, wie soeben gezeigt ist: der allen jenen n Gleichungen gemeinsame Komplex ist jetzt aber nicht die einzige Grösse ϱ^p, sondern der Komplex $\varrho^{rst\ldots} + \varrho^{2rst\ldots} + \ldots + \varrho^p$. Da dieser, sowie jeder zu subtrahirende und zu addirende Komplex $= 0$ ist; so folgt

$$B = 0 \qquad \text{und} \qquad Y = 0 \tag{51}$$

Hiernach ist z. B. für $p = 2, 3, 5, 7$, $30 = 2.3.5$, $70 = 2.5.7$, $105 = 3.5.7$ $Y = 1$, für $p = 6 = 2.3$, $15 = 3.5$, $210 = 2.3.5.7$ $Y = -1$, für $p = 4 = 2^2$, $9 = 3^2$, $12 = 2^2\,3$, $18 = 2.3^2$, $24 = 2^3.3$, $36 = 2^2\,3^2$ $Y = 0$.

Sind nun $b, c, d \ldots$ die zu p relativ primen Zahlen $< p$, deren Anzahl gleich m sein möge (indem man für $p = r^\alpha\, s^\beta\, t^\gamma \ldots$ bekanntlich $m = r^{\alpha-1}(r-1)\, s^{\beta-1}(s-1)\, t^{\gamma-1}(t-1) \ldots$ hat); so ergiebt sich aus der durch Division mit $x - 1$ in $x^p - 1$ entspringenden Gleichung $A = 0$ die Gleichung

$$x^b + x^c + x^d + \ldots = Y \tag{52}$$

Hat nun die Kongruenz $x^m \equiv 1 \bmod p$ primitive Wurzeln und ist a eine solche, nämlich eine Zahl, deren sukzessive Potenzen $a^1, a^2, a^3 \ldots a^m$ allen zu p relativen Zahlen als Resten nach dem Model p kongruent sind; so kann man die Exponenten $b, c, d \ldots$ durch diese Reste ersetzen und das frühere Verfahren in Anwendung bringen. Dasselbe wird die Zerlegung der Grundtafel von m Resten in Gruppen, deren Anzahl Faktoren von m sind, zum Zweck haben. Bezeichnet man die Grundtafel und die daraus gebildeten Gruppen wiederum mit $Y, P, Q, R \ldots$; so hat man jetzt zu beachten, dass Y den Werth aus Gl. (50) oder (51) hat und dass ein Glied, welches einem Reste b entspricht, der ein gemeinschaftliches Maass mit p hat, eine Grösse ϱ^b repräsentirt, deren Werth als bekannt vorausgesetzt, resp. durch Auflösung der Gleichungen (48) gefunden wird.

Den Fall, wo die Kongruenz $x^m \equiv 1 \bmod p$ keine primitive Wurzel hat, werden wir in Nr. 4 erörtern.

3) Beispielsweise ist für $p = 9 = 3^2$, wofür es 6 zu 9 relativ prime Zahlen 1, 2, 4, 5, 7, 8 giebt, $a = 2$ eine primitive Wurzel der Kongruenz $x^6 \equiv 1 \bmod 9$. Die Gleichungen (48) beschränken sich auf die eine

$$\varrho^3 + \varrho^6 + \varrho^9 = 0$$

und man hat als Grundtafel der Reste der sukzessiven Potenzen von 2

$$Y = 1 \quad 2 \quad 4 \quad 8 \quad 7 \quad 5$$

Zerlegt man diese sechsgliedrige Tafel in drei zweigliedrige Gruppen; so kömmt

$$P_1 = 1 \quad 8$$
$$P_2 = 2 \quad 7$$
$$P_3 = 4 \quad 5$$

Hiermit ist die Auflösung eigentlich schon vollbracht, da man nach der Formel (41) aus jeder zweigliedrigen Periode leicht eine Wurzel der Gleichung $x^p = 1$ herstellen kann und man im vorliegenden Falle auch keine solche Wurzel der Gleichung $x^9 = 1$ findet, welche zugleich der Gleichung $x^3 = 1$ angehört. Es kömmt also nur auf die Darstellung der drei Grössen P_1, P_2, P_3 an. Hierfür ist zunächst $P_1 + P_2 + P_3 = Y = 0$, sodann ist

$$P_1 P_2 = \varrho^3 + \varrho^6 + P_1 \quad P_2 P_3 = \varrho^3 + \varrho^6 + P_2 \quad P_3 P_1 = \varrho^3 + \varrho^6 + P_3$$
$$F(P_1 P_2) = 3(\varrho^3 + \varrho^6) + P_1 + P_2 + P_3 = -3$$
$$P_1 P_2 P_3 = \varrho^3 + \varrho^6 + P_1 + P_2 + P_3 = -1$$

Die kubische Gleichung, deren Wurzeln die Grössen P_1, P_2, P_3 sind, ist also

$$x^3 - 3x + 1 = 0$$

Wollte man die Grundtafel zuerst in zwei dreigliedrige Gruppen zerlegen; so hätte man

$$P_1 = 1 \quad 4 \quad 7$$
$$P_2 = 2 \quad 8 \quad 5$$
$$P_1 + P_1 = Y = 0 \text{ und } P_1 P_2 = 3(\varrho^3 + \varrho^6 + \varrho^9) = 0$$

folglich zur Bestimmung von P_1 und P_2 die quadratische Gleichung $x^2 = 0$, welche $P_1 = 0$ und $P_2 = 0$ ergiebt, wie es nach den Zeigern der Glieder dieser beiden Grössen auch ganz selbstverständlich ist, da $P_1 = \varrho^1 + \varrho^4 + \varrho^7 = \varrho(\varrho^0 + \varrho^3 + \varrho^6) = 0$ und ebenso $P_2 = \varrho^2 + \varrho^8 + \varrho^5 = \varrho^2(\varrho^0 + \varrho^3 + \varrho^6) = 0$ sein muss.

Zerlegt man jedes P in drei eingliedrige Q; so kömmt $Q_1 = 1$, $Q_2 = 4$, $Q_3 = 7$, $Q_4 = 2$, $Q_5 = 8$, $Q_6 = 5$. Für die Theilgruppen von P_1 ist $Q_1 + Q_2 + Q_3 = P_1 = 0$, $Q_1 Q_2 = 5 = Q_6$, $Q_2 Q_3 = 2 = Q_4$, $Q_1 Q_3 = 8 = Q_5$, also $(F(Q_1 Q_2) = Q_6 + Q_4 + Q_5 = P_2 = 0$, endlich $Q_1 Q_2 Q_3 = 3 = \varrho^3$. Ebenso hat man für die Theilgruppen von P_2 $Q_4 + Q_5 + Q_6 = P_2 = 0$, $F(Q_4 Q_5) = P_1 = 0$, $Q_4 Q_5 Q_6 = 6 = \varrho^6$. Die beiden kubischen Gleichungen resp. für Q_1, Q_2, Q_3 und für Q_4, Q_5, Q_6, welche zugleich die Werthe resp. von $\varrho^1, \varrho^4, \varrho^7$, $\varrho^2, \varrho^8, \varrho^5$ ergeben, sind hiernach $x^3 - \varrho^3 = 0$ und $x^3 - \varrho^6 = 0$. Wenn demzufolge ϱ^3 aus der quadratischen Gleichung $(\varrho^3)^0 + (\varrho^3)^1 + (\varrho^3)^2 = 0$ als

$$\varrho^3 = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$$

bestimmt ist, giebt die Auflösung der vorletzten Gleichung ϱ in der Form

$$x = \sqrt[3]{-\frac{1}{2} + \frac{1}{2}\sqrt{-3}}$$

4) Wenn die Kongruenz $x^m \equiv 1 \ mod\ p$ keine primitive Wurzel hat; so erinnern wir uns der schon in §. 1 gemachten Bemerkung, dass es für das in §. 5 entwickelte Verfahren nicht durchaus nothwendig ist, die Exponenten der Gleichung $x^{p-1} + x^{p-2} + \ldots + x = -1$ als die Reste der Potenzen einer einzigen Wurzel a darzustellen, dass es vielmehr nur darauf ankömmt, wenn mehrere Wurzeln $a, a_1, a_2 \ldots$ zu diesem Zwecke gewählt werden, dass die Potenzen jeder einzelnen eine Horizontalreihe der Grundtafel vertreten, d. h. dass die Reste der sukzessiven Potenzen einer jeden der Wurzeln a einen bestimmten aliquoten Theil der zu p relativ primen Zahlen vertreten und dass keine zwei dieser Gruppen denselben Rest enthalten.

So giebt es z. B. für $p = 15 = 3 \cdot 5$ die 8 zu 15 relativ primen Zahlen 1, 2, 4, 7, 8, 11, 13, 14, die Kongruenz $x^8 \equiv 1 \ mod\ 15$ hat aber keine primitive Wurzel, vielmehr kehrt in der Reihe der sukzessiven Potenzen jeder Zahl, welche kleiner als 15 ist, der Rest 1 oder ein anderer Rest bei einer niedrigeren, als der 7-ten Potenz wieder. Nun liefert aber von den zu 15 relativ primen Zahlen, welche überhaupt nur für eine Wurzel a in Betracht kommen können, die Wurzel $a_1 = 2$ die vier Reste 1, 2, 4, 8 und die Wurzel $a_2 = 7$ die vier Reste 1, 7, 4, 13, wovon der erste und dritte auch der Reihe der Reste der Wurzel a_1 angehört. Formiren wir nun die Grundtafel nach dem Schema

$$\begin{array}{cccc} a_1^{\,0} & a_1^{\,2} & a_1^{\,3} & a_1^{\,4} \\ a_2 a_1^{\,0} & a_2 a_1^{\,2} & a_2 a_1^{\,3} & a_2 a_1^{\,4} \end{array}$$

so erhält man die Grundtafel

$$\begin{array}{llllll} P_1 = & 1 & 2 & 4 & 8 \\ P_2 = & 7 & 14 & 13 & 11 \end{array}$$

Die Kombination von P_1 und P_2 giebt

$$P_1 P_2 = 4\,\varrho^0 + \varrho^3 + \varrho^6 + \varrho^9 + \varrho^{12} + + P_1 + P_2$$

oder da $\varrho^0 = 1$, $\varrho^0 + \varrho^3 + \varrho^6 + \varrho^9 + \varrho^{12} = 0$ und wegen $Y = -1$ $P_1 + P_2 = Y = -1$ ist, $P_1 P_2 = 2$. Hiernach finden sich die beiden Gruppen P_1 und P_2 aus der Gleichung

$$x^2 + x + 2 = 0$$

Dieselben sind also $\frac{1}{2} \mp \frac{1}{2}\sqrt{-7}$. Zerlegt man weiter; so kömmt

$$\begin{array}{llll} Q_1 = & 1 & 4 & \qquad Q_3 = 7 \quad 13 \\ Q_2 = & 2 & 8 & \qquad Q_4 = 14 \quad 11 \end{array}$$

also $Q_1 Q_2 = \varrho^3 + \varrho^6 + \varrho^9 + \varrho^{12} = -1$, $Q_3 Q_4 = \varrho^3 + \varrho^6 + \varrho^9 + \varrho^{12} = -1$. Die Grössen Q_1 und Q_2 ergeben sich daher aus der Gleichung $x^2 - P_1 x - 1 = 0$ und die Grössen Q_3 und Q_4 aus der Gleichung $x^2 - P_2 x - 1 = 0$; man hat also

$$Q_1 = \frac{1}{4}(1 + \sqrt{-7}) + \frac{1}{4}\sqrt{-6 + \sqrt{-7}}$$

$$Q_2 = \frac{1}{4}(1 + \sqrt{-7}) - \frac{1}{4}\sqrt{-6 + \sqrt{-7}}$$

$$Q_3 = \frac{1}{4}(1 - \sqrt{-7}) + \frac{1}{4}\sqrt{-6 - \sqrt{-7}}$$

$$Q_4 = \frac{1}{4}(1 - \sqrt{-7}) - \frac{1}{4}\sqrt{-6 - \sqrt{-7}}$$

Endlich ergiebt sich durch Zerlegung der Gruppen Q

$R_1 = 1$ $R_3 = 2$ $R_5 = 7$ $R_7 = 14$
$R_2 = 4$ $R_4 = 8$ $R_6 = 13$ $R_8 = 11$

mithin

$$R_1 R_2 = \varrho^5, \quad R_3 R_4 = \varrho^{10}, \quad R_5 R_6 = \varrho^5, \quad R_7 R_8 = \varrho^{10}$$

Die Werthe von ϱ^5 und ϱ^{10} ergeben sich aus der Gleichung $\varrho^0 + \varrho^5 + \varrho^{10} = 0$ oder $(\varrho^5)^2 + \varrho^5 + 1 = 0$ als $\varrho^5 = -\frac{1}{2} \mp \frac{1}{2}\sqrt{-3}$ und $\varrho^{10} = -\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$. Mit Hülfe dieser Werthe und der Werthe der Q findet sich R_1 und R_2 aus der Gleichung $x^2 - Q_1 x + \varrho^5 = 0$, ferner $R_3 R_4$ aus der Gleichung $x^2 - Q_2 x + \varrho^{10} = 0$, ferner $R_5 R_6$ aus $x^2 - Q_3 x + \varrho^5 = 0$ und R_7 und R_8 aus $x^2 - Q_4 x + \varrho^{10} = 0$.

In ähnlicher Weise kann man für $p = 30 = 2 \cdot 3 \cdot 5$, da es 8 zu 30 relativ prime Zahlen giebt, die Kongruenz $x^8 \equiv 1 \pmod{15}$ aber keine primitive Wurzel hat, $a_1 = 7$ und $a_2 = 17$ nehmen, sodass

$$P_1 = 1 \quad 7 \quad 19 \quad 13$$
$$P_2 = 17 \quad 29 \quad 23 \quad 11$$

und $Y = P_1 + P_2 = 1$ wird.

Für $p = 21 = 3 \cdot 7$ giebt es 12 zu 21 relativ prime Zahlen und die Kongruenz $x^{12} \equiv 1 \pmod{21}$ hat keine primitive Wurzel, man kann aber $a_1 = 5$ und $a_2 = 2$ setzen, wodurch man erhält

$$P_1 = 1 \quad 5 \quad 4 \quad 20 \quad 16 \quad 17$$
$$P_2 = 2 \quad 10 \quad 8 \quad 19 \quad 11 \quad 13$$

Für $p = 18 = 2 \cdot 3^2$ hat man 6 zu 18 relativ prime Zahlen und 5 ist eine primitive Wurzel von $x^6 \equiv 1 \pmod{18}$.

Für $p = 25 = 5^2$ giebt es 20 zu 25 relativ prime Zahlen und 2 ist eine primitive Wurzel von $x^{20} \equiv 1 \pmod{25}$.

Für $p = 24 = 2^3 \cdot 3$ sind 8 zu 24 relativ prime Zahlen 1, 5, 7, 11, 13, 17, 19, 23 vorhanden; die Kongruenz $x^8 \equiv 1 \pmod{24}$ hat keine primitive Wurzel und jede der sieben Zahlen 5, 7, 11, 13, 17, 19, 23 liefert nur zwei Potenzen, deren Reste verschieden sind. Man kann für die erste Horizontalreihe $a_1 = 5$ nehmen, wodurch dieselbe $P_1 = 1\ 5$ wird. Nimmt man für die zweite Reihe den Multiplikator $a_2 = 7$; so wird dieselbe $P_2 = 7\ 11$. Durch Multiplikation mit $a_3 = 13$ ergeben sich aus P_1 und P_2 die dritte und vierte Reihe $P_3 = 13\ 17$, $P_4 = 19\ 23$. Die Gesammttafel der Reste 1 5 7 11 13 17 19 23 hat den Werth $Y = 0$; es ist also $P_1 + P_2 + P_3 + P_4 = 0$. Für die zweidimensionalen Kombinationen erhält man

$P_1 P_2 = \varrho^8 + 2\varrho^{12} + \varrho^{16}$, $P_2 P_3 = 2\varrho^0 + \varrho^4 + \varrho^{20}$ u. s. w. und daher für die zweidimensionale symmetrische Funktion

$$\begin{aligned} F(P_1 P_2) &= 4\varrho^0 + \varrho^2 + 2\varrho^4 + 2\varrho^6 + 2\varrho^8 + \varrho^{10} + 4\varrho^{12} + \varrho^{14} \\ &\quad + 2\varrho^{16} + 2\varrho^{18} + 2\varrho^{20} + \varrho^{22} \\ &= (\varrho^0 + \varrho^2 + \varrho^4 + \ldots + \varrho^{22}) + 3(\varrho^0 + \varrho^{12}) + \varrho^4(\varrho^0 + \varrho^{12}) \\ &\quad + \varrho^6(\varrho^0 + \varrho^{12}) + \varrho^8(\varrho^0 + \varrho^{12}) \\ &= 0 \end{aligned}$$

Für die dreidimensionale symmetrische Funktion findet sich

$$\begin{aligned} F(P_1 P_2 P_3) &= 2(\varrho^3 + \varrho^9 + \varrho^{15} + \varrho^{21}) + 3Y \\ &= 2\varrho^3(\varrho^0 + \varrho^{12}) + 2\varrho^9(\varrho^0 + \varrho^{12}) + 3Y = 0 \end{aligned}$$

Die vierdimensionale Funktion wird

$$\begin{aligned} P_1 P_2 P_3 P_4 &= 6\varrho^0 + 3\varrho^4 + 2\varrho^{20} + \varrho^4(\varrho^0 + \varrho^{12}) + \varrho^8(\varrho^0 + \varrho^{12}) \\ &= 6\varrho^0 + 3\varrho^4 + 2\varrho^{20} = 6 + 3\varrho^4 - 3\varrho^8 \end{aligned}$$

Die Grössen P_1, P_2, P_3, P_4 bestimmen sich daher aus der biquadratischen Gleichung

$$x^4 + 6 + 3\varrho^4 - 3\varrho^8 = 0$$

worin wegen der Gleichung

$$\varrho^0 + \varrho^8 + (\varrho^8)^2 = 0 \quad \text{oder} \quad (\varrho^8)^2 + \varrho^8 = -1$$

$$\varrho^8 = -\frac{1}{2} + \frac{1}{2}\sqrt{-3} \quad \text{und} \quad \varrho^4 = \sqrt{-\frac{1}{2} + \frac{1}{2}\sqrt{-3}}$$

zu setzen ist. Die vier Wurzeln der letzteren biquadratischen Gleichung, welche die Werthe von P_1, P_2, P_3, P_4 darstellen, sind mithin, wenn man vor $\sqrt{-3}$ dasselbe Zeichen nimmt,

$$P = \sqrt[4]{-\frac{15}{2} \mp \frac{3}{2}\sqrt{-3} \pm 3\sqrt{-\frac{1}{2} \mp \frac{1}{2}\sqrt{-3}}}$$

Indem man jetzt $Q_1 = 1$, $Q_2 = 5$, $Q_3 = 7$, $Q_4 = 11$, $Q_5 = 13$, $Q_6 = 17$, $Q_7 = 19$, $Q_8 = 23$ setzt, wird für die ersten beiden Gruppen $Q_1 + Q_2 = P_1$ und $Q_1 Q_2 = \varrho^6 = \varrho^{12 \cdot \frac{1}{2}} = \sqrt{-1}$, mithin findet sich Q_1 und Q_2 aus der Gleichung

$$x^2 - P_1 x + \sqrt{-1} = 0$$

und hiernach ist

$$Q_1 = -\frac{1}{2}P_1 + \sqrt{\frac{1}{4}P_1^2 - \sqrt{-1}}$$

Wenn man hierin für P_1 den vorstehenden Werth substituirt, ist $Q_1 = \varrho_1$ oder die Seite des 24-eckes durch lauter Quadratwurzelausziehungen bestimmt.

Selbstverständlich kann man im letzten Beispiele die Grundtafel Y auch erst in zwei Gruppen 1 5 7 11 und 13 17 19 23, sowie auch in die zwei Gruppen 1 5 13 17 und 7 11 19 23 zerlegen, um sodann jede dieser Gruppen wiederum in zwei Gruppen und schliesslich jede der letzten Gruppen in zwei Elemente zu zerlegen.

5) Wenn p eine paare Zahl ist, hat die Gleichung $x^p - 1 = 0$ nicht nur die reelle Wurzel 1, sondern auch die reelle Wurzel -1, sie kann also durch Division mit $x^2 - 1$ sofort von diesen beiden reellen Wurzeln befreit werden. Das Resultat ist

$$x^{p-2} + x^{p-4} + x^{p-6} + \ldots + x^2 + 1 = 0$$

oder wenn man $x^2 = y$ und $\frac{1}{2}p = q$ setzt,

$$y^{q-1} + y^{q-2} + y^{q-3} + \ldots + y + 1 = 0$$

Um diese Gleichung wie früher die Gleichung $x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$ zu behandeln, hat man $q = \frac{p}{2}$ zum Model zu nehmen und für eine primitive Wurzel a der Kongruenz $x^{q-1} \equiv 1 \pmod{q}$ die Reste zu bilden, welche die Grundtafel Y bilden. So hätte man z. B. für das Achteck $p = 8$, $q = 4 = 2^2$, $Y = 0$ und, da 3 eine primitive Wurzel der Kongruenz $x^3 \equiv 1 \pmod{4}$ ist,

$$Y = 1 \quad 3$$

Indem man $P_1 = 1$, $P_2 = 3$ nimmt und die m-te Wurzel der Einheit mit σ, die p-te Wurzel aber wie vorhin mit ϱ bezeichnet und beachtet, dass $\sigma = \varrho^2$ ist, erhält man $P_1 + P_2 = Y = 0$, $P_1 P_2 = \sigma^4 = \varrho^8 = 1$. Hiernach ergeben sich die Werthe von P_1 und P_2 aus der Gleichung

$$x^2 + 1 = 0$$

und man hat also $P_1 = \sigma^1 = \varrho^2 = +\sqrt{-1}$ und $P_2 = \sigma^3 = \varrho^6 = -\sqrt{-1}$, mithin

$$\varrho = \sqrt{\sqrt{-1}} = e^{\frac{\pi}{4}\sqrt{-1}} \text{ und } \varrho^3 = \sqrt{-\sqrt{-1}} = e^{\frac{3\pi}{4}\sqrt{-1}}$$

wie es auch dem Achtecke entspricht.

Der Exponent $q - 1$ ist paar, wenn $p = 2(2n + 1)$ das Doppelte einer unpaaren Zahl ist; $q - 1$ ist dagegen unpaar, wenn $p = 4n$ ein Vielfaches von 4 ist, wie im letzten Beispiele $p = 8$. Im letzteren Falle hat die Gleichung $x^p - 1$ ausser den beiden reellen Wurzeln 1 und -1 auch die beiden imaginären Wurzeln $+\sqrt{-1}$ und $-\sqrt{-1}$. Wenn man dieselbe von den vier Wurzeln ± 1 und $\pm\sqrt{-1}$ durch Division mit $x^4 - 1$ befreiet, und nun $x^4 = y$, $\frac{1}{4}p = q$ setzt; so kömmt

$$x^{p-4} + x^{p-8} + \ldots + x^4 + 1 = 0$$

oder

$$y^{q-1} + y^{q-2} + \ldots + y + 1 = 0$$

So könnte man für $p = 8$, $q = 2$ die Gleichung $y + 1 = 0$ bilden, welche sofort die Auflösung $y = -1$, also $x = \sqrt[4]{-1}$ ergiebt.

Wenn allgemein $p = 2^\alpha q$ ist, worin q irgend eine unpaare Zahl ist; so hat die Gleichung $x^p - 1 = 0$ den Divisor $x^{2^\alpha} - 1 = 0$. Dividirt man mit demselben und setzt $x^{2^\alpha} = y$; so kömmt

$$y^{q-1} + y^{q-2} + \ldots + y + 1 = 0$$

worin der höchste Exponent $q - 1$ jedenfalls einen paaren Werth hat.

§. 10. Zurückführung der Periodengleichungen auf Gleichungen mit reellen Koeffizienten und Wurzeln.

Für einen unpaaren primen oder zusammengesetzten Werth von p hat die Gleichung $x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$ und für einen paaren Werth von p die in §. 9 Nr. 5 betrachtete Gleichung $y^{q-1} + y^{q-2} + \ldots + y + 1 = 0$ lauter komplexe Wurzeln. Demzufolge werden die aus Summen dieser Wurzeln bestehenden Perioden P, Q, R ... und die symmetrischen Funktionen derselben zum Theil komplexe Werthe annehmen; man wird also bei dem in §. 5 bis 10 erörterten Verfahren auf Gleichungen mit komplexen Koeffizienten und Wurzeln stossen. Dem kann man entgehen, d. h. man kann die Auflösung auf lauter Gleichungen mit reellen Koeffizienten und Wurzeln zurückführen, wenn man die Gleichung $x^{p-1} + \ldots + x + 1 = 0$ oder die Gleichung $y^{q-1} + \ldots + y + 1 = 0$, worin $q - 1$ paar, die Gliederzahl also unpaar ist, durch $a^{\frac{1}{2}(p-1)}$, resp. $a^{\frac{1}{2}(q-1)}$ dividirt, das mittelste Glied transponirt, darauf je zwei von beiden Enden her gleich weit abstehende Glieder zusammenfasst und wie in §. 2 das Binom $x^b + x^{-b}$, resp. $y^b + y^{-b}$ mit X_b bezeichnet; denn hierdurch erhält man; indem man $\frac{1}{2}(p-1)$ oder $\frac{1}{2}(q-1)$ gleich m setzt, die Gleichung

$$X_1 + X_2 + X_3 + \ldots + X_m = -1$$

welche ganz so wie die Gl. (3) in §. 2 behandelt werden kann. Zu diesem Ende kommen für die Zeiger 1, 2, 3 ... m nur die kleinsten absoluten Reste einer primitiven Wurzel der Kongruenz $x^{p-1} \equiv 1 \bmod p$, resp. der Kongruenz $x^{q-1} \equiv 1 \bmod q$ ohne Rücksicht auf ihr Zeichen in Betracht, man hat jedoch zu beachten, dass jetzt die Kombinationen zweier Perioden wie P_1 und P_2, welche durch das Produkt $P_1 P_2$ repräsentirt sind, nicht aus den Summen der betreffenden Reste, sondern aus den Summen und Differenzen dieser Reste ohne Rücksicht auf das Zeichen bestehen und dass die hierbei sich ergebenden Nullreste nach §. 5 Nr. 11 die Grösse $x^0 + x^{-0}$ oder $y^0 + y^{-0}$, also den Werth 2 vertreten.

Jedes X hat offenbar einen reellen Werth und demzufolge können in deren Perioden und symmetrischen Funktionen keine komplexen Grössen

erscheinen, alle entstehenden Gleichungen werden also reelle Koeffizienten und reelle Wurzeln enthalten.

Bei diesem Verfahren erhält die Grundtafel nur halbso viel Reste als früher und eine Zerlegung fällt weg, indem dafür zuletzt die quadratische Gleichung von der Form $z + \frac{1}{z} = c$ an die Stelle tritt. Ausserdem ist es jetzt nicht unbedingt nothwendig, dass a eine primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \ mod\ p$ sei; es genügt, wenn alle kleinsten absoluten Reste von $a^0, a^1, \ldots a^{m-1}$ verschieden sind oder alle Zahlen $1, 2 \ldots m$ enthalten.

Beispielsweise ist für das Siebeneck $p = 7 = 2 \cdot 3 + 1$ und man erhält statt der Gleichung $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$ die Gleichung

$$X_1 + X_2 + X_3 = -1$$

Obgleich die Zahl 2 keine primitive Wurzel nach 7 ist, kann man dieselbe doch für a nehmen, weil ihre ersten drei Potenzen $2^0, 2^1, 2^2$ resp. die kleinsten Reste 1, 2, 3 nach dem Model 7 haben. Hiernach hat man $P_1 = 1$, $P_2 = 2$, $P_3 = 3$, also $P_1 + P_2 + P_3 = Y = -1$, $P_1 P_2 = 3, 1$, $P_2 P_3 = 2, 1$, $P_1 P_3 = 3, 2$, also $F(P_1 P_2) = 2\ (1, 2, 3) = 2\ Y = -2$, ferner $P_1 P_2 P_3 = (P_1 P_2) \times P_3 = 1, 3, 0, 2 = P(0) + Y = 2 - 1 = 1$. Hiernach finden sich die drei Grössen P_1, P_2, P_3, welche zugleich die drei Grössen X_1, X_2, X_3 sind, als die reellen Wurzeln der Gleichung

$$x^3 + x^2 - 2x - 1 = 0$$

Jeder Werth von X liefert dann zwei Seiten des Siebeneckes nach der Formel

$$\varrho = \frac{1}{2} X \mp \sqrt{\frac{1}{4} X^2 - 1}$$

§. 11. Aufsuchung der primitiven Wurzeln.

1) Zur Auflösung der Gleichung $x^p = 1$, worin wir p als Primzahl voraussetzen, ist die Kenntniss einer primitiven Wurzel der Kongruenz $x^{p-1} \equiv 1 \ mod\ p$ erforderlich. Wenn $r, s, t \ldots$ die verschiedenen Primfaktoren von $p - 1$ sind; so ergiebt das bekannte Verfahren, von den Zahlen $1, 2, 3 \ldots p - 1$ alle diejenigen auszuschliessen, welche Reste von Potenzen der Grade $r, s, t \ldots$ sind (vergl. Serret, Cours d'algèbre supérieure, 24me leçon) alle primitiven Wurzeln. Obgleich das Verfahren sehr einfach ist, so ist es doch bei grossen Werthen von p sehr mühsam, und allgemeine Merkmale zur sofortigen Erkennung solcher Wurzeln werden daher immer erwünscht sein. Zu dem Ende erinnern wir an den ebenfalls bekannten Satz, dass die Anzahl der primitiven Wurzeln gleich der Anzahl der zu $p - 1$ relativ primen Zahlen $b, c, d \ldots$, welche $< p - 1$ sind (einschliesslich der Zahl 1) ist und dass, wenn a irgend eine dieser Wurzeln ist, alle Wurzeln durch die Reste der Potenzen $a^b, a^c, a^d \ldots$ dargestellt sind.

Um eine Wurzel a auf ihre Primitivität zu prüfen, brauchte man, wenn $r, s, t \ldots m$ die verschiedenen einfachen und zusammengesetzten Faktoren von $p-1$ sind, sodass $m = \frac{p-1}{2}$ den grössten derselben bezeichnet, nur die Reste der Potenzen $a^r, a^s, a^t \ldots a^m$ zu kennen. Ist irgend einer dieser Reste $= 1$; so ist a keine primitive Wurzel. Jedenfalls muss für eine primitive Wurzel der Rest von a^m gleich $p-1$ oder, wenn man negative Werthe zulässt, gleich -1 sein. Angenommen nun, es sei eine niedrigere Potenz von a als die m-te, etwa die Potenz $a^r \equiv 1$; so muss r ein Faktor von $p-1$ oder $p-1 = rs$ und alle Potenzen $a^r, a^{2r}, a^{3r} \ldots a^{sr}$ müssen $\equiv 1$ sein. Da aber $a^m \equiv -1$ und jeder Rest, also auch der Rest -1 sich in Abständen von r aufeinanderfolgenden Potenzen wiederholt; so müssen die Potenzen $a^{\frac{r}{2}}, a^{\frac{3r}{2}}, a^{\frac{5r}{2}}, \ldots a^{\frac{(2s-1)r}{2}} \equiv -1$ sein und es muss in Abständen von $\frac{1}{2}r$ Gliedern ein Zeichenwechsel vor sich gehen, sodass man

$$\begin{array}{cccccccccc} & a^0 & a^{\frac{r}{2}} & a^r & a^{\frac{3r}{2}} & a^{2r} & \ldots & a^n & \ldots & a^{rs} \\ \equiv & 1 & -1 & 1 & -1 & 1 & \ldots & -1 & \ldots & 1 \end{array}$$

hat.

Letzteres ist nur möglich, wenn r paar und s unpaar ist. Die Nothwendigkeit der Paarheit von r leuchtet sofort ein: wäre aber bei einem paaren r der Faktor s ebenfalls paar, also $m = \frac{1}{2}rs = 2.\frac{r}{2}.\frac{s}{2}$; so könnte a^m, als eine gerade Potenz von $a^{\frac{r}{2}}$ oder von -1, nicht $\equiv -1$ sein.

Hieraus folgt zunächst, dass wenn $p-1$ überhaupt keine unpaaren, sondern nur paare Faktoren hat, wenn also $p = 2^\alpha + 1$ ist, jede Zahl a, für welche $a^m \equiv -1$ ist, eine primitive Wurzel ist.

Was die unpaaren Werthe von s betrifft; so ist, weil $p-1$ eine paare Zahl ist, mit jedem derselben ein paares r verbunden, also die eine Vorbedingung erfüllt. Die Primitivität der Wurzel a verlangt also, dass für keinen in $p-1$ enthaltenen unpaaren Faktor s die Potenz $a^{\frac{r}{2}} \equiv -1$ oder $a^r \equiv 1$ sei. Übrigens brauchen für s nur die in $p-1$ enthaltenen Primfaktoren untersucht zu werden. Denn setzt man $p-1 = rs = rs's'' = r''s''$, indem $s = s's''$, $r'' = rs'$ ist, und nimmt man an, dass $a^{\frac{r}{2}} \equiv -1$ sei; so wird auch, weil s' unpaar ist, $a^{\frac{rs'}{2}} = a^{\frac{r''}{2}} \equiv -1$: kann also die letztere Kongruenz für den einfachen Faktor s'' nicht stattfinden; so ist auch die erstere für den zusammengesetzten Faktor s nicht möglich. Hiernach erfordert eine primitive Wurzel a, dass keine Potenz $a^{\frac{r}{2}} = a^{\frac{p-1}{2s}}$, worin s alle in $p-1$ enthaltenen unpaaren Primfaktoren darstellt, $\equiv -1$ oder keine Potenz $a^{\frac{p-1}{s}} \equiv 1$ sei.

Mit Zuhülfenahme des Reziprozitätsgesetzes führen die vorstehenden Bedingungen zu folgenden Sätzen.

2) Wenn die Primzahl $p = 2^\alpha + 1$ ist, also $p - 1$ nur den Primfaktor 2 enthält; so ist jeder quadratische Nichtrest nach p (also jede Zahl a, für welche $a^n \equiv -1 \mod p$ ist), eine primitive Wurzel nach p, und jeder quadratische Rest nach p (also jede Zahl a, für welche $a^n \equiv 1 \mod p$ ist), keine primitive Wurzel nach p. Hieraus folgt:

a) Die Zahl 2 ist eine primitive Wurzel, wenn die eben charakterisirte Primzahl p zugleich die Form $8n + 3$ oder $8n + 5$ hat. Die erste Form ist nur für $p = 3$ und die zweite nur für $p = 5$ möglich: demnach ist 2 eine primitive Wurzel nach 3 und auch nach 5, jedoch nicht nach $p = 17, 257$ etc.

b) Die Zahl -2 oder $p - 2$ ist eine primitive Wurzel, wenn p die Form $8n + 5$ oder $8n + 7$ hat. Die erste Form findet nur für $p = 5$ statt, sodass $5 - 2 = 3$ eine primitive Wurzel nach 5 ist: die Form $8n + 7$ kann nicht stattfinden.

c) Da mit Ausnahme der kleinsten Primzahl 3 von der Form $2^\alpha + 1$ jede grössere Primzahl dieser Art $\equiv 2 \mod 3$ oder $\equiv -1 \mod 3$, also ein quadratischer Nichtrest nach dem Model 3 ist; so muss nach dem Fundamentalsatze 3 ein Nichtrest nach p sein. Demzufolge ist 3 eine primitive Wurzel nach p mit alleiniger Ausnahme des Falles $p = 3$, also für alle diejenigen Primzahlen wie 5, 17, 257 etc., welche eine konstruirbare Kreistheilung ermöglichen.

3) Angenommen, es sei die Primzahl $p = 2q + 1$ und q eine beliebige Primzahl; so sind alle Nichtreste nach p mit alleiniger Ausnahme des Nichtrestes -1 oder $p - 1$ primitive Wurzeln nach p. Wenn also p die Form $8n + 3$ hat, ist 2, wenn p die Form $8n + 5$ hat, ist 2 und auch -2 oder $p - 2$, und wenn p die Form $8n + 7$ hat, ist -2 oder $p - 2$ eine primitive Wurzel nach p. Hätte p die Form $8n + 1$; so würde weder 2, noch $p - 2$ eine primitive Wurzel nach p sein: dieser Fall kann jedoch nicht stattfinden und auch der Fall $p = 8n + 5$ ist nur für die einzige Primzahl $p = 5 = 2 \cdot 2 + 1$, nämlich für den Fall möglich, wo q die paare Primzahl 2 ist. Für einen unpaaren Werth von q, wo also p die Form $8n + 3$ oder $8n + 7$ hat, ist daher 2, resp. $p - 2$ eine primitive Wurzel. So ist z. B. für $p = 11 = 2 \cdot 5 + 1$ und $p = 59 = 2 \cdot 29 + 1$, da p die Form $8n + 3$ hat, die Zahl 2 eine primitive Wurzel, für $p = 7 = 2 \cdot 3 + 1$, $p = 23 = 2 \cdot 11 + 1$, $p = 47 = 2 \cdot 23 + 1$, da p die Form $8n + 7$ hat, ist dagegen die Zahl -2 oder resp. 5, 21, 45 eine primitive Wurzel.

4) Da jede primitive Wurzel a nach p ein quadratischer Nichtrest sein muss; so ist es wichtig, Merkmale der quadratischen Nichtreste, sowie Merkmale derjenigen Nichtreste, welche keine primitiven Wurzeln sind, also ausgeschlossen werden müssen, zu konstatiren.

Jede Zahl a ist quadratischer Nichtrest nach p, für welche $a^{\frac{p-1}{2}} \equiv -1 \mod p$ ist. Für den speziellen Werth $a = 2$ fassen wir

die bekannten Sätze, dass die $\frac{p-1}{2}$-te Potenz von 2 den Rest 1 hat, wenn p die Form $8r + 1$ oder $8r + 7$ besitzt, dagegen den Rest -1, wenn p die Form $8r + 3$ oder $8r + 5$ hat, in den einen Satz zusammen, dass allgemein

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \mod p$$

ist. Jede Potenz der Zahl 2 von paarem Grade, also $a = 2^{2n}$ ist ein quadratischer Rest, da $\left(2^{2n}\right)^{\frac{p-1}{2}} = \left(2^{p-1}\right)^n \equiv 1 \mod p$ ist. Für jede Potenz der Zahl 2 von unpaarem Grade, also $a = 2^{2n+1}$ hat man dagegen

$$\left(2^{2n+1}\right)^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \mod p$$

Für $a = -2$ erhält man

$$(-2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{(p+5)(p-1)}{8}} \mod p$$

Setzt man links -2^{2n} für -2; so kömmt

$$\left(-2^{2n}\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p$$

und setzt man -2^{2n+1} für -2,

$$\left(-2^{2n+1}\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{(p+5)(p-1)}{8}} \mod p$$

a) Hiernach ist für die Primzahlen von der Form $8r + 3$ und $8r + 5$, also z. B. für 3, 5, 11, 13, 19, 29 etc. sowohl 2, als auch 8, als auch 32 etc. ein quadratischer Nichtrest. Ausserdem ist -2, -8, -32 etc. oder $p - 2$, $p - 8$, $p - 32$ etc. quadratischer Nichtrest für die Primzahlen von der Form $8r + 5$ und $8r + 7$, also für 5, 7, 13, 23, 29 etc., während -4, -16, -64 etc. oder $p - 4$, $p - 16$, $p - 64$ etc. quadratischer Nichtrest für die Primzahlen von der Form $4r + 3$, z. B. für 3, 7, 11, 19, 23 etc. ist.

Wenn a eine unpaare Primzahl ist, und man setzt

$$a^{\frac{p-1}{2}} \equiv (-1)^m \mod p \qquad p^{\frac{a-1}{2}} \equiv (-1)^n \mod a$$

so muss $m + n = \frac{p-1}{2} \cdot \frac{a-1}{2}$, oder da a ein quadratischer Nichtrest oder $m = 1$ sein soll,

$$n = \frac{p-1}{2}\,\frac{a-1}{2} - 1$$

sein. Setzt man $-a$ für a; so hat man die Bedingungen

$$(-a)^{\frac{p-1}{2}} \equiv (-1)^{m'} \equiv (-1)^{\frac{p-1}{2}+m} \mod p \qquad p^{\frac{a-1}{2}} \equiv (-1)^n \mod a$$

$$m' + n = \frac{p-1}{2} \cdot \frac{a+1}{2}$$

und, dann $m' = 1$ sei,

$$n = \frac{p-1}{2} \cdot \frac{a+1}{2} - 1$$

(Für einen quadratischen Rest a müsste $m = 0$, also $n = \frac{p-1}{2}\frac{a-1}{2}$ und für einen quadratischen Rest $-a$ müsste $n = \frac{p-1}{2}\frac{a+1}{2}$ sein.)

Kann man nun für gewisse Werthe von a die Grösse n anderweit bestimmen; so liefert die vorstehende Gleichung ein Kennzeichen für den quadratischen Nichtrest a. Nimmt man einmal $a = 3$, also $\frac{a-1}{2} = 1$; so kann p entweder $= 3x + 1 \equiv 1 \ mod\ 3$, oder es kann $= 3x + 2 \equiv -1 \ mod\ 3$ sein. Im ersten Falle, für $p = 3x + 1$, ist $p^{\frac{a-1}{2}} = p \equiv 1 \equiv (-1)^0 \ mod\ 3$, also $n = 0$ eine paare Zahl, oder p ein quadratischer Rest nach 3, und 3 wird ein Nichtrest nach p sein, wenn zugleich der Ausdruck $n = \frac{p-1}{2} \cdot \frac{a-1}{2} - 1 = \frac{3x}{2} - 1$ eine paare Zahl darstellt. Letzteres geschieht, wenn $\frac{3x}{2}$ unpaar oder x paar und $= 4r + 2$, mithin $p = 12r + 7$ ist. Im zweiten Falle, für $p = 3x + 2$ ist $p^{\frac{a-1}{2}} = p \equiv 2 \equiv (-1)^1 \ mod\ 3$, also $n = 1$ eine unpaare Zahl oder p ein quadratischer Nichtrest nach 3, und 3 wird ein Nichtrest nach p sein, wenn $n = \frac{p-1}{2} \cdot \frac{a-1}{2} - 1 = \frac{3x+1}{2} - 1$ eine unpaare Zahl wird. Diess geschieht wenn x unpaar und $= 4r + 1$, mithin $p = 12r + 5$ ist.

b) Hiernach ist 3 ein quadratischer Nichtrest für jede Primzahl von der Form $12r + 5$, wie 5, 17, 29, 41, 53, 89 etc. und von der Form $12r + 7$, wie 7, 19, 31, 43 etc., aber für keine Primzahl von der Form $12r + 1$, wie 13, 37, 61 etc., oder von der Form $12r + 11$, wie 11, 23, 47 etc., indem 3 für diese ein quadratischer Rest ist.

Nimmt man $a = 5$, also $\frac{a-1}{2} = 2$; so kann p eine der vier Formen $5x + 1$, $5x + 2$, $5x + 3$, $5x + 4$ haben. Im ersten und vierten Falle ist $p^{\frac{a-1}{2}} = p^2 \equiv 1 \ mod\ 5 \equiv (-1)^0$, also $n = 0$ eine paare Zahl oder p ein quadratischer Rest nach 5, und 5 wird ein Nichtrest nach p sein, wenn zugleich der Ausdruck $n = \frac{p-1}{2} \cdot \frac{a-1}{2} - 1 = p - 2$ eine paare Zahl ist, was unmöglich ist. Im zweiten und dritten Falle ist $p^{\frac{a-1}{2}} = p^2 \equiv -1 \ mod\ 5$, also $n = 1$ eine unpaare Zahl oder p ein quadratischer Nichtrest nach 5, und 5 wird ein Nichtrest nach p sein, wenn zugleich der Ausdruck $n = \frac{p-1}{2} \cdot \frac{a-1}{2} - 1 = p - 2$

eine unpaare Zahl ist. Da Letzteres unbedingt der Fall ist; so hat man den Satz:

c) Die Zahl 5 ist ein quadratischer Nichtrest für jede Primzahl von der Form $5r + 2$, wie 7, 17, 37 etc., und von der Form $5r + 3$, wie 13, 23, 43 etc., aber für keine Primzahl von der Form $5r + 1$ und $5r + 4$, indem sie für diese ein quadratischer Rest ist.

Nimmt man $a = 7$, also $\frac{a-1}{2} = 3$; so kann p eine der sechs Formen $7x + 1$, $7x + 2$, $7x + 3$, $7x + 4$, $7x + 5$, $7x + 6$ haben. Für dieselben hat man $p^{\frac{a-1}{2}} = p^3$ resp. $\equiv (-1)^0$, $(-1)^0$, (-1), $(-1)^0$, (-1), (-1), also n resp. $= 0, 0, 1, 0, 1, 1$. Hiernach wird 7 ein quadratischer Nichtrest nach p sein, wenn zugleich der Ausdruck $n = \frac{p-1}{2}\frac{a-1}{2} - 1 = 3.\frac{p-1}{2} - 1$ resp. paar, paar, unpaar, paar, unpaar, unpaar wird. Diess geschieht resp. für $x = 4r + 2$, $4r + 3$, $4r + 2$, $4r + 1$, $4r$, $4r + 1$ und liefert den Satz:

d) Die Zahl 7 ist ein quadratischer Nichtrest für jede Primzahl von irgend einer der Formen $28r + 5$, $28r + 11$, $28r + 13$, $28r + 15$, $28r + 17$, $28r + 23$, also z. B. für die Primzahlen 5, 61, 11, 67, 13, 41, 43, 17, 73, 23, 79 etc., aber für keine Primzahl von der Form $28r + 1$, $28r + 3$, $28r + 9$, $28r + 19$, $28r + 25$, $28r + 27$, indem sie für diese ein quadratischer Rest ist.

5) Wir generalisiren die zuletzt behandelten Fälle, indem wir unter a eine beliebige unpaare Primzahl denken und alsdann die Primzahl p in den $a - 1$ verschiedenen Formen $ax + 1$, $ax + 2$, $ax + 3$, ... $ax + (a-1)$ vorstellen. Bezeichnet dann α irgend eine der Zahlen $1, 2, 3 \ldots (a-1)$, welche ein quadratischer Rest nach dem Model a ist, und β irgend eine dieser Zahlen, welche ein quadratischer Nichtrest nach a ist, sodass man also für $p = ax + \alpha \equiv \alpha \bmod a$

$$p^{\frac{a-1}{2}} \equiv \alpha^{\frac{a-1}{2}} \equiv (-1)^0 \bmod a \quad \text{oder} \quad n = 0$$

und für $p = ax + \beta \equiv \beta \bmod a$

$$p^{\frac{a-1}{2}} \equiv \beta^{\frac{a-1}{2}} \equiv -1 \bmod a \quad \text{oder} \quad n = 1$$

hat; so erfordert die Bedingung, dass a ein quadratischer Nichtrest nach p sei, im ersten, resp. zweiten Falle, dass $\frac{p-1}{2} \cdot \frac{a-1}{2}$ resp. unpaar oder paar, dass also

$$\frac{ax + \alpha - 1}{2} \cdot \frac{a-1}{2} \quad \text{unpaar}$$

eventuell

$$\frac{ax + \beta - 1}{2} \cdot \frac{a-1}{2} \quad \text{paar}$$

sei. Jenachdem man nun für a Werthe von der Form $4u + 1$ und $4u + 3$, für α und β aber Werthe von der Form $4v$, $4v + 1$, $4v + 2$, $4v + 3$ (welche zum Theil in den Formen $2v$ und $2v + 1$ vereinigt

sind) substituirt, zeigt sich, dass p die aus nachstehender Tafel ersichtliche Form haben muss.

a	α	p	a	β	p
			$4u+1$	$2v$	$(2r+1)a+\beta$
				$2v+1$	$2ra+\beta$
$4u+3$	$4v$	$(4r+1)a+\alpha$	$4u+3$	$4v$	$(4r+3)a+\beta$
	$4v+1$	$2(2r+1)a+\alpha$		$4v+1$	$4ra+\beta$
	$4v+2$	$(4r+3)a+\alpha$		$4v+2$	$(4r+1)a+\beta$
	$4v+3$	$4ra+\alpha$		$4v+3$	$2(2r+1)a+\beta$

Diese Tafel sagt unter Anderem:

a) Eine Primzahl a von der Form $4u+1$ kann niemals ein Nichtrest für eine unpaare Primzahl von der Form $ra+\alpha$ sein, sie ist aber ein Nichtrest für jede Primzahl $(2r+1)a+\beta$, wenn β paar ist, und für jede Primzahl $2ra+\beta$, wenn β unpaar ist. Eine jede Primzahl a von der Form $4u+3$ ist ein Nichtrest für jede Primzahl resp. von der Form $(4r+1)a+\alpha$, $2(2r+1)a+\alpha$, $(4r+3)a+\alpha$, $4ra+\alpha$, jenachdem α die Form $4v$, $4v+1$, $4v+2$, $4v+3$ hat, auch ist sie ein Nichtrest für jede Primzahl von der Form $(4r+3)a+\beta$, $4ra+\beta$, $(4r+1)a+\beta$, $2(2r+1)a+\beta$, jenachdem β die Form $4v$, $4v+1$, $4v+2$, $4v+3$ hat.

b) Die Zahl 1 gehört immer zu den quadratischen Resten nach a, vertritt also den Werth $\alpha = 4v+1$. Daraus folgt, dass eine Primzahl a von der Form $4u+3$ ein Nichtrest nach jeder Primzahl von der Form $2(2r+1)a+1$ ist.

c) Die Zahl -1 vertritt einen Werth von β. Eine Primzahl a von der Form $4u+1$ ist ein Nichtrest nach jeder Primzahl von der Form $2ra-1$ und eine Primzahl a von der Form $4u+3$ ist ein Nichtrest nach jeder Primzahl $2(2r+1)a-1$.

d) Die Zahl $a+1$ ist ein Vertreter von α. Eine Primzahl a von der Form $4u+3$ ist ein Nichtrest nach jeder Primzahl $2(2r+1)a+1$.

e) Die Zahl $a-1$ ist ein Vertreter von β. Eine Primzahl a von der Form $4u+1$ ist ein Nichtrest nach jeder Primzahl $2ra-1$ und eine Primzahl a von der Form $4u+3$ ist ein Nichtrest nach jeder Primzahl $2(2r+1)a-1$.

6) Wenngleich uns für die obigen Zwecke vornehmlich die quadratischen Nichtreste nach der Primzahl p interessiren und die quadratischen Reste die von den Nichtresten ausgeschlossenen Formen haben; so ist es doch nützlich, auch die Merkmale der quadratischen Reste kurz anzuführen. Bei der vorstehenden Bezeichnung wird a ein quadratischer Rest nach $p = ax+\alpha$, resp. $ax+\beta$ sein, wenn

$$\frac{ax+\alpha-1}{2}\cdot\frac{a-1}{2} \quad \text{paar}$$

eventuell $\frac{ax+\beta-1}{2} \cdot \frac{a-1}{2}$ unpaar

ist. Diess giebt folgende Tafel:

a	u	p	a	β	p
$4u+1$	$2v$	$(2r+1)a+u$			
	$2v+1$	$2ra+u$			
$4u+3$	$4v$	$(4r+3)a+u$	$4u+3$	$4v$	$(4r+1)a+\beta$
	$4v+1$	$4ra+u$		$4v+1$	$2(2r+1)a+\beta$
	$4v+2$	$(4r+1)a+u$		$4v+2$	$(4r+3)a+\beta$
	$4v+3$	$2(2r+1)a+u$		$4v+3$	$4ra+\beta$

a) Hiernach ist eine Primzahl a von der Form $4u+1$ niemals ein quadratischer Rest für eine unpaare Primzahl von der Form $ra+\beta$, sie ist aber ein Rest für jede Primzahl von der Form $(2r+1)a+u$, wenn u paar ist, und für jede Primzahl von der Form $2ra+u$, wenn u unpaar ist. Eine jede Primzahl von der Form $4u+3$ ist ein quadratischer Rest für jede Primzahl resp. von der Form $(4r+3)a+u$, $4ra+u$, $(4r+1)a+u$, $2(2r+1)a+u$, jenachdem u die Form $4v$, $4v+1$, $4v+2$, $4v+3$ hat, auch ist sie ein Rest für jede Primzahl von der Form $(4r+1)a+\beta$, $2(2r+1)a+\beta$, $(4r+3)a+\beta$, $4ra+\beta$, jenachdem β die Form $4v$, $4v+1$, $4v+2$, $4v+3$ hat.

b) Die Zahl 1 gehört immer zu den quadratischen Resten nach a, kann also einen Werth von u vertreten. Eine Primzahl a von der Form $4u+1$ ist ein quadratischer Rest nach jeder Primzahl von der Form $2ra+1$ und eine Primzahl a von der Form $4u+3$ ist ein quadratischer Rest nach jeder Primzahl von der Form $4ra+1$.

c) Die Zahl -1 vertritt einen Werth von β. Eine Primzahl a von der Form $4u+3$ ist ein quadratischer Rest nach jeder Primzahl von der Form $4ra-1$.

d) Die Zahl $a+1$ ist ein Vertreter von u. Eine Primzahl a von der Form $4u+1$ ist ein quadratischer Rest nach jeder Primzahl von der Form $2ra+1$ und eine Primzahl a von der Form $4u+3$ ist ein Rest nach jeder Primzahl von der Form $4ra+1$.

e) Die Zahl $a-1$ ist ein Vertreter von β. Eine Primzahl a von der Form $4u+3$ ist ein quadratischer Rest nach jeder Primzahl von der Form $4ra-1$.

7. Die in Nr. 4 bis 6 betrachteten quadratischen Nichtreste sind nicht sämmtlich primitive Wurzeln nach p, vielmehr sind von jenen Nichtresten a diejenigen auszuschliessen, für welche eine Potenz, deren Exponent $r < \frac{p-1}{2}$ ist, $\equiv \pm 1 \ mod\ p$ ist. Offenbar kommen für r nur Faktoren

von $\frac{p-1}{2}$ in Betracht, also Werthe, für welche $rs = \frac{p-1}{2}$ ist. Der Fall $a^r \equiv 1 \ mod\ p$ kann nicht eintreten, da derselbe die Kongruenz $a^{rs} \equiv 1 \ mod\ p$ bedingt, welche der Voraussetzung widerspricht. Es ist daher nur der Fall $a^r \equiv -1 \ mod\ p$ zu untersuchen. Es leuchtet ein, dass der zweite Faktor s nothwendig unpaar sein muss: denn wäre er paar; so würde $a^{rs} \equiv (-1)^s \equiv 1 \ mod\ p$ sein und könnte nicht, wie verlangt, $\equiv -1$ sein. Hiernach muss r alle in $\frac{p-1}{2}$ etwa enthaltenen Potenzen von 2 in sich aufnehmen: ist also $p = (2^\alpha u^\beta v^\gamma w^\delta \ldots) + 1$ und $\frac{p-1}{2} = 2^{\alpha-1} u^\beta v^\gamma \ldots$, worin $u, v \ldots$ unpaare Primzahlen bezeichnen; so können für s nur die Werthe $u, v, w \ldots$, also für r nur die Werthe $2^{\alpha-1} u^{\beta-1} v^\gamma w^\delta \ldots$, $2^{\alpha-1} u^\beta v^{\gamma-1} w^\delta \ldots$, $2^{\alpha-1} u^\beta v^\gamma w^{\delta-1} \ldots$ angenommen werden: denn jeder andere Werth r', welcher für r anzunehmen wäre, ist ein Faktor von einem der vorstehenden r. Wäre nun für ein solches r' $a^{r'} \equiv -1$; so wäre auch $a^r \equiv -1$: die Untersuchung kann sich also auf die letzteren Werthe von r beschränken.

Beispielsweise kömmt es für die Primzahl $p = 6301 = 2^2 . 3^2 . 5^2 . 7 + 1$ darauf an, von den quadratischen Nichtresten a diejenigen auszuschliessen, für welche $r = 2 . 3 . 5^2 . 7$, $2 . 3^2 . 5 . 7$, oder $2 . 3^2 . 5^2$ ist, d. h. diejenigen, für welche entweder die $(2 . 3 . 5^2 . 7)$-te, oder die $(2 . 3^2 . 5 . 7)$-te, oder die $(2 . 3^2 . 5^2)$-te Potenz $\equiv -1 \ mod\ p$ ist. Um Diess für irgend ein a zu untersuchen, wird man erst den Rest b der Potenz $2 . 3 . 5$ bilden und aus diesem Reste die Reste von b^3, b^5, um schliesslich aus diesen Resten die Reste von $(b^3)^7$, $(b^5)^7$, $(b^5)^3$ darzustellen und nachzusehen, ob sich unter den letzteren der Rest -1 oder $p-1$ befindet.

Die Untersuchung wird umso einfacher, je einfacher die Zusammensetzung von $p-1$ ist. Ist $p-1$ das Produkt aus einer beliebigen Potenz von 2 und der ersten Potenz einer Primzahl q also $p = 2^\alpha q + 1$; so sind von den quadratischen Nichtresten a nur diejenigen auszuschliessen, für welche $a^{2^{\alpha-1}} \equiv -1 \ mod\ p$ ist, (insofern nicht gerade $2^{\alpha-1} = \frac{p-1}{2}$ würde, was nur für eine Primzahl von der Form $p = 2^\alpha + 1$, wofür $q = 1$ ist, also für eine hier gar nicht in Betracht kommende Primzahl geschehen kann). Beispielsweise ist nach Nr. 4, b die Zahl 3 ein quadratischer Nichtrest jeder Primzahl p von der Form $12r + 5$. Von diesen Primzahlen haben $29 = 2^2 . 7 + 1$, $41 = 2^3 . 5 + 1$, $53 = 2^2 . 13 + 1$, $89 = 2^3 . 11 + 1$ die Form $2^\alpha q + 1$; es müsste also für die erste, zweite, dritte, vierte der Nichtrest 3 ausgeschlossen werden, insofern $3^2 = 9 \equiv -1 \ mod\ 29$, $3^1 = 81 \equiv -1 \ mod\ 41$, $3^2 = 9 \equiv -1 \ mod\ 53$, $3^4 = 81 \equiv -1 \ mod\ 89$ wäre. Diess trifft nur für $p = 41$, nicht für $p = 29, 53, 89$ zu, und demzufolge ist 3 **eine primitive Wurzel** für jede dieser Primzahlen **29, 53, 89**, jedoch nicht für die Primzahl 41.

Hat p die Form $2q^\beta + 1$; so sind nur die Potenzen $a^{q^{\beta-1}}$, also für $p = 2q^2 + 1$ nur die Potenzen a^q zu prüfen (der Fall $p = 2q + 1$ ist schon durch Nr. 3 erledigt). So ist z. B. $19 = 2 . 3^2 + 1$, und da

19 auch die Form $12r + 7$ hat; so ist 3 nach Nr. 4, b ein Nichtrest nach 19, insofern nach Vorstehendem nicht $3^3 = 27 \equiv -1 \ mod\ 19$ ist. Da Letzteres nicht der Fall ist; so ist 3 eine primitive Wurzel für die Primzahl 19.

Hat p die Form $2qs + 1$, worin q, s zwei Primzahlen auf erster Potenz bezeichnen; so sind die Potenzen a^q und a^s zu untersuchen. Beispielsweise ist $31 = 2 . 3 . 5 + 1$ und, da 31 auch die Form $12r + 7$ hat; so ist 3 nach Nr. 4, b ein Nichtrest nach 31, falls nicht 3^3 oder $3^5 \equiv -1 \ mod\ 31$ ist. Da Letzteres nicht der Fall ist; so ist 3 eine primitive Wurzel für die Primzahl 31. Serret ermittelt die primitiven Wurzeln für 31 in der 24-sten Vorlesung seiner Algèbre supérieure. Eine Vergleichung jenes Verfahren mit dem vorstehenden bringt die grosse Kürze des letzteren zur Anschauung.

Der Satz in Nr. 4, c lehrt zugleich, dass, weil 31 die Form $5r + 1$ hat, die Zahl 5 keine primitive Wurzel für 31 sein kann. Ebenso lehrt der Satz in Nr. 4, d dass, weil 31 die Form $28r + 3$ hat, die Zahl 7 keine primitive Wurzel für 31 sein kann.

Nach dem Satze Nr. 5, e ist 7 ein Nichtrest nach jeder Primzahl von der Form $14(2r + 1) - 1$, also z. B. nach $97 = 14 . 7 - 1$. Da $97 = 2^5 . 3 + 1$ ist; so ist der Rest von $7^{2^4} \equiv 7^{16} \ mod\ 97$ zu prüfen. Da derselbe nicht gleich -1 ist; so ist 7 eine primitive Wurzel für 97.

8) Wenn in $p = (2^\alpha u^\beta v^\gamma w^\delta \ldots) + 1$ u die grösste und w die kleinste der ungeraden Primzahlen $u, v, w \ldots$ ist; so wird $2^{\alpha-1} u^\beta v^\gamma w^{\delta-1}$ der grösste der in Betracht kommenden Werthe von r sein. Ist nun die Primzahl a so klein, dass

$$a^r < p \quad \text{also} \quad a < \sqrt[r]{p}$$

ist; so kann keine der in Frage kommenden Potenzen von a den Rest -1 haben: es brauchen also für solche Werthe von a oder auch für solche Werthe von p, welche $> a^r$ sind, keine Potenzen von a geprüft zu werden, vielmehr ist für solche Werthe eine jede Primzahl a, welche quadratischer Nichtrest nach p ist, auch eine primitive Wurzel nach p.

Praktisch wird dieser Satz vornehmlich bei Primzahlen von der Form $p = 2^\alpha u + 1$, indem dann $r = 2^{\alpha-1}$ ist. So ist z. B. für $p = 53 = 8 . 6 + 5$ nach Nr. 4, a die Zahl 2 ein Nichtrest. Da zugleich $p = 2^2 . 13 + 1$ und demnach $r = 2$, aber $2^2 < 53$ ist; so ist 2 ohne Weiteres eine primitive Wurzel nach 53. Nach Nr. 4, a ist auch -2 oder $53 - 2 = 51$ eine primitive Wurzel. Nach Nr. 4, b ist auch 3 ein quadratischer Nichtrest nach 53 und, weil $3^2 < 53$ ist, zugleich eine primitive Wurzel nach 53. Nach Nr. 4, c ist auch 5 ein quadratischer Nichtrest und weil $5^2 < 53$ ist, eine primitive Wurzel nach 53. Dagegen ist nach Nr. 4, d die Zahl 7 kein Nichtrest, mithin auch keine primitive Wurzel nach 53.

Im Allgemeinen kommen für den Exponenten r mehrere Werthe in Frage: von allen diesen können nach Vorstehendem diejenigen Werthe

unberücksichtigt bleiben, welche $< \frac{\log p}{\log a}$ oder auch $< \frac{\log (p-1)}{\log a}$ sind. So hat man z. B. in dem obigen Beispiele für $p = 31$ die beiden Reste von 3^3 und 3^5 zu untersuchen, wovon der erste sofort zu übersehen und nur der zweite zu prüfen ist. Für $p = 239 = 2 \cdot 7 \cdot 17 + 1 = 29 \cdot 8 + 7$ ist nach Nr 4, a die Zahl -2 ein Nichtrest und es sind die beiden Potenzen $(-2)^7 = -2^7$ und $(-2)^{17} = -2^{17}$ zu prüfen. Da $2^7 < 239$ ist, kömmt sie nicht in Betracht, und da für die zweite $2^{17} \equiv 108 \ mod\ 239$, also nicht $\equiv -1$ ist; so ist -2 oder $239 - 2 = 237$ eine primitive Wurzel nach 239.

§. 12. Die geometrische Konstruktion der Gleichungen und namentlich der regelmässigen Polygone.

1) Um eine quadratische Gleichung geometrisch zu konstruiren, pflegt man sie aufzulösen und die Konstruktion dem Ausdrucke, welcher die Auflösung darstellt, anzupassen. Ich habe jedoch in dem „Situationskalkul“ §. 9 gezeigt, dass dieses Verfahren der Konstruktion nach arithmetischen Auflösungen durchaus nicht dem Geiste der Geometrie entspricht, dass vielmehr im echt geometrischen Sinne geometrische Örter in Form von Linien und Flächen nach Gesetzen oder Funktionen, welche unaufgelös'te Gleichungen darstellen, darzustellen sind, deren Durchschnitte die gesuchten Auflösungen liefern. So haben wir bereits in §. 3 die Konstruktion des regelmässigen Dreieckes, Fünfeckes und Siebzehneckes, überhaupt des p-eckes für die Primzahlen von der Form $p = 2^a + 1$ auf die Konstruktion der unaufgelös'ten Gleichungen zweiten Grades zurückgeführt. Das dabei befolgte Prinzip besteht darin, anstatt die Gleichung

$$x^2 + ax + b = 0$$

für die Unbekannte x aufzulösen und nach dem allgemeinen arithmetischen Ausdrucke für x dessen beide Werthe x_1 und x_2 geometrisch darzustellen, die beiden Gleichungen

$$x_1 + x_2 = -a \qquad x_1 x_2 = b$$

mit den zwei Unbekannten x_1 und x_2 in unaufgelös'ter Form zu behandeln, nämlich einen Kreis als den Ort der Endpunkte zweier Vektoren x_1 und x_2 mit konstantem Produkte $x_1 x_2$, ferner eine gerade Linie als Ort der Endpunkte zweier Vektoren von konstanter Summe $x_1 + x_2$ darzustellen und deren Durchschnitte zu bilden.

Ein demselben Grundgedanken entsprechendes Verfahren ist auch dasjenige, welches bei der graphischen Darstellung der reellen Wurzel einer höheren Gleichung $f(x) = 0$ in Anwendung gebracht wird, indem man x als die Abszisse einer Kurve $y = f(x)$ betrachtet und die Durchschnitte dieser Kurve mit der Abszissenaxe, nämlich mit der Linie $y = 0$ sucht.

2) Da die Koeffizienten a_1, a_2, a_3 ... der Gleichung n-ten Grades

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n = 0$$

die symmetrischen Funktionen F der Wurzeln x_1, x_2 ... x_n darstellen; so geben die Beziehungen

$$F_1 = -a_1 \qquad F_2 = a_2 \qquad F_3 = -a_3 \quad \text{etc.}$$

Gelegenheit, verschiedene Linien- und Flächenörter darzustellen, deren gemeinschaftliche Durchschnitte die Wurzeln x_1, x_2 ... sind.

3) Für die Gleichung zweiten Grades ergiebt sich hierdurch ausser den beiden soeben erwähnten Konstruktionen die folgende. Sieht man die eine der beiden Wurzeln x_1, x_2, etwa x_1 als die Abszisse und die andere x_2 als die Ordinate einer Kurve an; so ergeben die Werthe der beiden symmetrischen Funktionen

$$x_1 + x_2 = -a_1 \qquad x_1 x_2 = a_2$$

die beiden Kurven

$$x_2 = -x_1 - a_1 \qquad x_2 = \frac{a_2}{x_1}$$

Die zweite stellt eine gleichseitige Hyperbel dar, deren reelle Axe sich unter 45^0 gegen die Grundaxe OX neigt und an welcher die Koordinatenaxen OX und OY Asymptoten bilden. Die erste stellt eine gerade Linie dar, welche mit der reellen Axe der Hyperbel parallel läuft. Beide Linien schneiden sich in zwei Punkten, und die Abszisse und Ordinate des einen dieser beiden Punkte stellt die beiden Wurzeln x_1, x_2 dar. Welcher von den beiden Durchschnittspunkten der gesuchte ist, entscheidet sich leicht durch die Zeichen von a_1 und a_2.

4) Für die Gleichung dritten Grades hat man

$$x_1 + x_2 + x_3 = -a_1 \qquad x_1 x_2 + x_2 x_3 + x_1 x_3 = a_2 \qquad x_1 x_2 x_3 = -a_3$$

Setzt man

$$x_2 x_3 = y_1 \qquad x_2 + x_3 = y_2$$

so erhält man die Beziehungen

$$x_1 = -a_1 - y_2 = \frac{a_2 - y_1}{y_2} = -\frac{a_3}{y_1}$$

Die Gleichung

$$y_1 = -\frac{a_3}{x_1}$$

stellt eine gleichseitige Hyperbel dar, an welcher die Abszissen- und Ordinatenaxe Asymptoten sind; x_1 ist die Abszisse, y_1 die Ordinate. Die aus den ersten beiden Beziehungen sich ergebende Gleichung

$$y_1 = x_1^2 + a_1 x_1 + a_2$$

stellt eine Parabel dar, deren Axe mit der Ordinatenaxe OY parallel läuft, indem x_1 die Abszisse und y_1 die Ordinate bezeichnet. Diese Parabel schneidet jene Hyperbel in drei Punkten, deren Koordinaten je zwei zusammengehörige Werthe von x_1 und y_1 repräsentiren. Jeder Werth von x_1 liefert sofort eine Wurzel der gegebenen kubischen Gleichung.

Wenden wir diese Regel auf das Siebeneck an; so ist nach §. 10 $a_1 = 1$, $a_2 = -2$, $a_3 = -1$. Die Hyperbel $y_1 = \frac{1}{x_1}$ hat die Halbaxen $\sqrt{2}$, und ihre reelle Axe neigt sich unter 45^0 gegen die positive Abszissenaxe OX. Ist in Fig. 15 O der Anfangspunkt der Koordinatenaxen OX, OY und $OC = CA$ die Längeneinheit; so ist $OA = OB = \sqrt{2}$ die reelle Halbaxe dieser Hyperbel. Die Parabel $y_1 = x_1^2 + x_1 - 2$ hat den Parameter $\frac{1}{2}$ und, wenn $OD = \frac{1}{2}$, $DE = \frac{9}{4}$ ist, ihren Scheitel in E. Schneiden sich beide Kurven in den Punkten F_1, F_2, F_3; so sind die Abszissen OG_1, OG_2, OG_3 die Vertreter der drei Wurzeln x_1, x_2, x_3 der gegebenen kubischen Gleichung. Dieselben repräsentiren, wenn ϱ_1, ϱ_2, ϱ_3 die erste, zweite, dritte Seite und ϱ_{-1}, ϱ_{-2}, ϱ_{-3} die sechste, fünfte, vierte Seite des Siebeneckes bezeichnen, die Grössen

$$X_1 = \varrho_1 + \varrho_{-1} \qquad X_2 = \varrho_2 + \varrho_{-2} \qquad X_3 = \varrho_3 + \varrho_{-3}$$

und sie stellen sich in der Zeichnung in richtiger Reihenfolge dar. Errichtet man also in den Endpunkten der Abszissen OG_1, OG_2, OG_3 Perpendikel und schneiden dieselben einen um den Mittelpunkt O mit dem Radius $OH_0 = 2$ beschriebenen Kreis oberhalb der Abszissenaxe in den drei Punkten H_1, H_2, H_3 und unterhalb in den drei Punkten H_6, H_5, H_4; so sind OH_0, OH_1, OH_2, OH_3, OH_4, OH_5, OH_6 die Radien des regelmässigen Siebeneckes $H_0 H_1 H_2 H_3 H_4 H_5 H_6$ in dem Kreise vom Radius 2. Die Wurzel x_3 stellt zugleich den Abstand OG_3 der Seite des Siebeneckes vom Mittelpunkte O und der zugehörige Werth von y_3 die Länge der halben Seite $G_3 H_4$ dar.

5) Will man die Durchschnitte von Flächen zulassen; so repräsentirt

$$x_1 = -\frac{a_3}{x_2 x_3}$$

die Ordinate und x_2, x_3 die unabhängig veränderlichen Abszissen einer krummen Fläche, welche aus vier Zweigen besteht, an den die drei Koordinatenebenen XOY, YOZ, ZOX Asymptotenebenen bilden. Die Gleichung

$$x_1 = \frac{a_2 - x_2 x_3}{x_2 + x_3}$$

stellt eine Fläche zweiten Grades dar, für welche x_1, x_2, x_3 die Bedeutung wie für die erste Fläche haben. Die Gleichung

$$x_1 = -a_1 - x_2 - x_3$$

endlich stellt eine Ebene mit der nämlichen Bedeutung der Grössen x_1, x_2, x_3 dar. Diese Ebene schneidet die Durchschnittslinie der ersten beiden Flächen in Punkten, deren Koordinaten zusammengehörige Werthe der drei Wurzeln x_1, x_2, x_3 sind. Die Merkmale desjenigen dieser Punkte, welcher der einzig zulässige ist, sind leicht zu finden.

Wenngleich die Grössen x_1, x_2, x_3 nach dem letzteren Verfahren nicht geometrisch, d. h. nicht mit den in der niederen Geometrie gestatteten Hülfsmitteln von Lineal und Zirkel konstruirbar sind; so

ist dieses Verfahren doch insofern interessant, als es mit einem Schlage die drei Wurzeln einer kubischen Gleichung als die Koordinaten einunddesselben Punktes im Raume erscheinen lässt, auch die Werthe der Koeffizienten a_1, a_2, a_3 oder symmetrischen Funktionen der Wurzeln zur unmittelbaren Anschauung bringt. Wenn man das den drei rechtwinkligen Kanten x_1, x_2, x_3 entsprechende Parallelepipedum beschreibt; so ist die symmetrische Funktion dritten Grades $x_1 x_2 x_3 = -a_3$ der ganze kubische Inhalt desselben, die symmetrische Funktion zweiten Grades $x_1 x_2 + x_2 x_3 + x_1 x_3 = a_2$ ist die Hälfte der Oberfläche desselben, die symmetrische Funktion ersten Grades $x_1 + x_2 + x_3 = -a_1$ ist der vierte Theil der Kantenlänge oder des linearen Umfanges desselben, und die symmetrische Funktion vom Grade null, nämlich der Koeffizient 1 des ersten Gliedes der kubischen Gleichung ist der achte Theil der Anzahl der Eckpunkte desselben. Hiernach involvirt die Auflösung der kubischen Gleichung die Bestimmung eines Parallelepipedums, dessen kubischer Inhalt, Oberfläche, Kantenlänge und Eckzahl gegeben ist, und das letztere Verfahren stellt dieses Parallelepipedum unmittelbar dar.

6) Die Gleichung vierten Grades lässt sich ebenfalls durch die Durchschnittspunkte dreier Flächen darstellen. Denn die vier Beziehungen

$$x_1 + x_2 + x_3 + x_4 = -a_1 \quad x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_1 + x_1 x_3 + x_2 x_4 = a_2$$

$$x_1 x_2 x_3 + x_2 x_3 x_4 + x_3 x_4 x_1 + x_4 x_1 x_2 = -a_3 \qquad x_1 x_2 x_3 x_4 = a_4$$

liefern, wenn man $x_1 x_2 = y_1$, $x_1 + x_2 = y_2$, $x_3 + x_4 = y_3$ setzt, die drei Gleichungen

$$y_1 y_3 + \frac{a_4 y_2}{y_1} = -a_3$$

$$y_1 + \frac{a_4}{y_1} + y_2 y_3 = a_2$$

$$y_2 + y_3 = -a_1$$

oder auch

$$y_2 - \frac{y_1}{a_4}(a_3 + y_1 y_3) = \frac{a_2 y_1 - y_1^2 - a_4}{y_1 y_3} = -a_1 - y_3$$

Die ersten beiden Gleichungen stellen krumme Flächen, die dritte eine Ebene dar, welche mit der Axe der y_1 parallel läuft oder auf der Ebene der $y_2 y_3$ normal steht. Der Durchschnitt dieser Ebene mit der Durchschnittskurve jener beiden Flächen ergiebt zusammengehörige Werthe von y_1, y_2, y_3, welche mittelst der zuerst aufgestellten Beziehungen zur Kenntniss der Wurzeln x_1, x_2, x_3, x_4 führen.

7) Von grösserer Wichtigkeit als die übrigen Resultate ist das in Nr. 4 enthaltene. Dasselbe lehrt, dass jedes regelmässige Polygon, dessen Seitenzahl eine Primzahl p von der Form $2^\alpha 3^\beta + 1$ ist, mittelst Kegelschnitte konstruirbar ist, wenn man das in §. 10 beschriebene Verfahren in Anwendung bringt, welches nur Gleichungen mit reellen Koeffizienten und reellen Wurzeln liefert. Zu diesen Polygonen gehört unter Anderem das 7-eck, das 13-eck, das 19-eck, das 37-eck,

das 73-eck, das 97-eck. Nach §. 9 erweisen sich mit denselben Mitteln auch die Polygone konstruirbar, deren Seitenzahl eine zusammengesetzte Zahl von der Form $2^\alpha 3^\beta$ ist, unter Anderem also (ausser dem 3-ecke, dem 6-ecke, dem 12-ecke etc.) auch das 9-eck, das 18-eck, das 27-eck, das 36-eck.

Da der Kreis und die gerade Linie ebenfalls Kegelschnitte sind; so gestattet die niedere Geometrie zu ihren Hülfsmitteln zwei Spezialitäten von Kegelschnitten. Zu dieser Beschränkung liegt überall kein zwingender Grund vor, da sich jeder Kegelschnitt aus gegebenen Bestimmungsstücken mittelst geeigneter Instrumente ebenso sicher verzeichnen lässt, als ein Kreis mittelst des Zirkels und eine gerade Linie mittelst des Lineals. Die Bedingungen der euklidischen Geometrie sind unzulängliche Postulate, welche auf keine ausschliessliche Geltung Anspruch haben: wenn man von denselben absieht, muss man sagen, das Siebeneck, das Dreizehneck, das Neuneck, das Neunzehneck und viele andere regelmässige Polygone sind ebenso gut konstruirbar wie das Dreieck, das Fünfeck, das Siebzehneck.

8) Um eine Vorstellung von der Möglichkeit eines Kegelschnittzirkels zu geben; so sei in Fig. 16 die ebene horizontale Platte AB, auf welcher ein Kegelschnitt mit der in die Linie AB fallenden Axe verzeichnet werden soll, im Punkte C durchbohrt. In dem Bohrloche C sei eine Stange DE aufundnieder zu schieben und in der Vertikalebene AFB drehbar, sodass sie unter jedem Winkel $FCB = \alpha$ gegen die Platte geneigt und sodann festgestellt werden kann. Um den Punkt F der Stange DE ist ein Schreibstift GFH drehbar und verschiebbar. Derselbe ist zunächst in der Ebene AFB oder CFG drehbar, sodass dem Winkel CFG jeder Werth β gegeben und sodann der Stift GFH in dieser Neigung gegen die Stange DE festgehalten werden kann, ohne jedoch seine Wälzbarkeit um die Stange DE und seine Verschiebbarkeit in der Richtung GFH zu beeinträchtigen. Wird jetzt der Stift GFH um die Stange DE herumgeführt und mit der Spitze G auf der Platte gehalten; so beschreibt diese Spitze in stetigem Zuge einen Kegelschnitt und zwar eine Ellipse, wenn $\alpha > \beta$ ist, ferner eine Parabel, wenn $\alpha = \beta$ ist, und endlich eine Hyperbel, wenn $\alpha < \beta$ ist, in welchem letzteren Falle die vordere Spitze G des Stiftes den einen Zweig und die hintere Spitze H den anderen Zweig der Hyperbel verzeichnet.

IV. Die Theilbarkeit der Zahlen von der Form $2^r + 1$.

§. 13. Zerlegung dieser Zahlen.

1) Legendre hielt jede Zahl p von der Form $2^r + 1$, worin der Exponent r von 2 selbst eine Potenz von 2 ist, für eine Primzahl. Dieser Satz erwies sich als ein Irrthum, nachdem Euler bemerkt hatte, dass

die Zahl $2^{32} + 1 = 4\,294\,967\,297$ durch 641 theilbar, nämlich $= 641 \cdot 6\,700\,417$ ist. Euler wird diese Entdeckung vermuthlich durch Probedivisionen mit den aufsteigenden Primzahlen gemacht haben, und dieses Verfahren führte in dem gegebenen Falle bald zu einem Resultate, da 641 zu den kleinen Primzahlen gehört. Hätte der Zufall es gewollt, dass p das Produkt aus zwei nahezu einander gleichen Primzahlen war; so wären etwa 5000 Divisionen mit allen Primzahlen unter 65 500 auszuführen gewesen, eine Arbeit, welcher sich nicht leicht ein Rechner unterziehen wird.

Bis jetzt ist nur ein Kriterium für eine Primzahl p bekannt, nämlich der Wilsonsche Lehrsatz, welcher sagt, dass das Produkt

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv -1 \mod p$$

sein müsse. Ein Produkt von 4000 Millionen Faktoren, selbst wenn von den sukzessiven Produkten auch immer nur die Reste nach p genommen werden, würde aber die Zeit von ungefähr 3000 Menschenleben in Anspruch nehmen, also absolut unausführbar sein.

Unter diesen Umständen mögen einige Sätze, welche unter gewissen Umständen für grosse Werthe von $p = 2^r + 1$ die Entscheidung, ob p eine Primzahl sei oder nicht, durch einfachere Mittel herbeizuführen im Stande sind, nicht ohne Nutzen sein.

2) Zunächst ist klar, dass wenn r eine unpaare Zahl ist, wie in $p = 2 + 1$, $2^3 + 1$, $2^5 + 1$ u. s. w. p stets den Faktor 3 hat, ferner, dass wenn r das Doppelte einer ungeraden Zahl ist, wie in $p = 2^2 + 1$, $2^6 + 1$, $2^{10} + 1$ u. s. w., p stets den Faktor 5 hat, allgemein aber, dass wenn $r = (2m + 1)n$ einen unpaaren Faktor $2m + 1$ hat, während der andere Faktor n paar oder unpaar sein mag, p stets den Faktor $2^n + 1$ besitzt, indem man

$$(1) \quad 2^{(2m+1)n} + 1 = (2^n + 1)\,(2^{2mn} - 2^{(2m-1)n} + 2^{(2m-2)n} - \ldots + 1)$$

hat. So ist z. B. $2^3 + 1 = 9$ ein Faktor von $2^3 + 1$, $2^9 + 1$, $2^{15} + 1$ u. s. w. und $2^4 + 1 = 17$ ist ein Faktor von $2^4 + 1$, $2^{12} + 1$, $2^{20} + 1$ u. s. w.

3) Hiernach ist jede Zahl $p = 2^r + 1$, deren Exponent r einen unpaaren Faktor hat, eine zusammengesetzte und eine Zahl von der Form $2^r + 1$ kann nur dann eine Primzahl sein, wenn r lauter paare Faktoren hat, also eine Potenz von 2 ist.

4) Unter den letzteren Zahlen können jedoch auch zusammengesetzte vorkommen. Um gewisse Merkmale derselben zu entdecken, kann man sich einmal die Frage vorlegen, wie, wenn ein Faktor in der Form $1 + 2^\alpha + 2^\beta + \ldots$ gegeben ist, der zweite Faktor $1 + 2^\gamma + 2^\delta + \ldots$ beschaffen sein muss, damit das Produkt beider die Form $1 + 2^r$ annehme. Der Satz Nr. 2 beantwortet diese Frage für den Fall, dass der erste Faktor $1 + 2^n$ sei, dahin, dass wenn für einen beliebigen Werth von m als zweiter Faktor die Zahl $1 - 2^n + 2^{2n} - 2^{3n} + \ldots + 2^{2mn}$ genommen wird, das Produkt gleich $1 + 2^{(2m+1)n}$ die verlangte Form hat, worin jedoch der Exponent von 2 einen unpaaren Faktor besitzt.

5) Bei der Untersuchung der Faktoren, welche eine Summe von mehreren Potenzen von 2 darstellen, leistet die Beziehung

$$(2) \quad (2^\alpha + 2^{\alpha+n})\,(2^m - 2^{m+n} + 2^{m+2n} - \ldots \mp 2^{m+rn}) = 2^{\alpha+m} \mp 2^{\alpha+m+(r+1)n}$$

welche das Produkt eines Binoms und Polynoms als die Summe der Produkte der beiden ersten und der beiden letzten Glieder darstellt, nützliche Dienste.

Diese Beziehung enthält unmittelbar die Formel

$$(1 + 2^n)\,(1 - 2^n + 2^{2n} - 2^{3n} + \ldots + (-1)^r\, 2^{rn}) = 1 + (-1)^r\, 2^{(r+1)n}$$

Für $r = 2m$ hat man die Formel (1). Indem man darin $n = 1, 2, 3 \ldots$ setzt, kömmt

$$\begin{aligned}
(1 + 2)\,(1 - 2 + 2^2 - 2^3 + \ldots + 2^{2m}) &= 1 + 2^{2m+1}\\
(1 + 2^2)\,(1 - 2^2 + 2^4 - 2^6 + \ldots + 2^{4m}) &= 1 + 2^{2(2m+1)}\\
(1 + 2^3)\,(1 - 2^3 + 2^6 - 2^9 + \ldots + 2^{6m}) &= 1 + 2^{3(2m+1)}\\
(1 + 2^4)\,(1 - 2^4 + 2^8 - 2^{10} + \ldots + 2^{8m}) &= 1 + 2^{4(2m+1)}
\end{aligned}$$

Hiernach ist $1 + 2 = 3$ ein Faktor jeder der Zahlen $1 + 2$, $1 + 2^3$ $1 + 2^5$, $1 + 2^7$ u. s. w., ferner ist $1 + 2^2 = 5$ ein Faktor jeder der Zahlen $1 + 2^2$, $1 + 2^6$, $1 + 2^{14}$, $1 + 2^{22}$, $1 + 2^{30}$ u. s. w., ferner $1 + 2^3 = 9$ ein Faktor jeder der Zahlen $1 + 2^3$, $1 + 2^9$, $1 + 2^{15}$, $1 + 2^{21}$, $1 + 2^{27}$ u. s. w., ferner $1 + 2^4 = 17$ ein Faktor jeder der Zahlen $1 + 2^4$, $1 + 2^{12}$, $1 + 2^{20}$, $1 + 2^{28}$ u. s. w.

Fasst man den neben $(1 + 2^n)$ stehenden Faktor ins Auge und setzt darin für jede Differenz wie $-2^m + 2^n$ den gleichwerthigen Ausdruck $2^m + 2^{m+1} + 2^{m+2} + \ldots + 2^{n-1}$; so zeigt sich, dass

$$1 + (2^n + 2^{n+1} + \ldots + 2^{2n-1}) + (2^{3n} + 2^{3n+1} + \ldots + 2^{4n-1}) + \ldots + (2^{(2r-1)n} + 2^{(2r-1)n+1} + \ldots + 2^{2rn-1})$$

wofür man auch

$$1 + 2^n\,(1 + 2^1 + 2^2 + \ldots + 2^{n-1})\,(1 + 2^{2n} + 2^{4n} + \ldots + 2^{2(r-1)n})$$

schreiben kann, ein Faktor von $1 + 2^{(2r+1)n}$ ist. Demnach ist für $n = 1, 2, 3 \ldots$

$$\begin{aligned}
1 + 2 + 2^2 + 2^5 + \ldots + 2^{2r-1} &= 1 + 2\,(1 + 2^2 + 2^4 + \ldots + 2^{2(r-1)})\\
1 + 2^2 + 2^3 + 2^6 + 2^7 + \ldots + 2^{4r-2} + 2^{4r-1} &\\
= 1 + 2^2\,(1 + 2)\,(1 + 2^4 + 2^8 + \ldots + 2^{4(r-1)}) &\\
1 + 2^3 + 2^4 + 2^5 + 2^9 + 2^{10} + 2^{11} + \ldots + 2^{6r-3} + 2^{6r-2} + 2^{6r-1} &\\
= 1 + 2^3\,(1 + 2 + 2^2)\,(1 + 2^6 + 2^{12} + \ldots + 2^{6(r-1)}) &
\end{aligned}$$

u. s. w. ein Faktor resp. von $1 + 2^{2r+1}$, $1 + 2^{2(2r+1)}$, $1 + 2^{3(2r+1)}$ etc. Für $r = 1, 2, 3 \ldots$ ergeben diese Formeln, dass

$$\begin{aligned}
1 + 2 &= 1 + 2 &&= 3 \text{ in } 1 + 2^2\\
1 + 2 + 2^3 &= 1 + 2\,(1 + 2^2) &&= 11 \text{ in } 1 + 2^5\\
1 + 2 + 2^3 + 2^5 &= 1 + 2\,(1 + 2^2 + 2^4) &&= 43 \text{ in } 1 + 2^7
\end{aligned}$$

u. s. w.

$1 + 2^2 + 2^3 = 1 + 2^2(1 + 2) = 13 \text{ in } 1 + 2^6$
$1 + 2^2 + 2^3 + 2^6 + 2^7 = 1 + 2^2(1 + 2)(1 + 2^4) = 205 \text{ in } 1 + 2^{10}$
$1 + 2^2 + 2^3 + 2^6 + 2^7 + 2^{10} + 2^{11} = 1 + 2^2(1 + 2)(1 + 2^4 + 2^8) = 3277 \text{ in } 1 + 2^{14}$
u. s. w.
$1 + 2^3 + 2^4 + 2^5 = 1 + 2^3(1 + 2 + 2^2) = 57 \text{ in } 1 + 2^9$
$1 + 2^3 + 2^4 + 2^5 + 2^9 + 2^{10} + 2^{11} = 1 + 2^3(1 + 2 + 2^2)(1 + 2^6) = 3641 \text{ in } 1 + 2^{15}$
$1 + 2^3 + 2^4 + 2^5 + 2^9 + 2^{10} + 2^{11} + 2^{15} + 2^{16} + 2^{17}$
$= 1 + 2^3(1 + 2 + 2^2)(1 + 2^6 + 2^{12}) = 223017 \text{ in } 1 + 2^{21}$
u. s. w.
enthalten ist.

Die Formel

(3) $(1 + 2^n + 2^{2n-1})(1 - 2^n + 2^{2n-1}) = 1 + 2^{2(2n-1)}$

lehrt, dass jede Zahl von der Form $1 + 2^n + 2^{2n-1}$ oder auch von der Form $1 - 2^n + 2^{2n-1}$ ein Faktor einer Zahl von der Form $1 + 2^{2(2n-1)}$ ist, und man hat für $n = 1, 2, 3 \ldots$

$1 + 2^2 = (1 + 2 + 2)(1 - 2 + 2) = 5 \cdot 1$
$1 + 2^6 = (1 + 2^2 + 2^3)(1 - 2^2 + 2^3) = 13 \cdot 5$
$1 + 2^{10} = (1 + 2^3 + 2^5)(1 - 2^3 + 2^5) = 41 \cdot 25$
$1 + 2^{14} = (1 + 2^4 + 2^7)(1 - 2^4 + 2^7) = 145 \cdot 113$
$1 + 2^{18} = (1 + 2^5 + 2^9)(1 - 2^5 + 2^9) = 545 \cdot 481$
$1 + 2^{22} = (1 + 2^6 + 2^{11})(1 - 2^6 + 2^{11}) = 2113 \cdot 1985$
$1 + 2^{26} = (1 + 2^7 + 2^{13})(1 - 2^7 + 2^{13}) = 8321 \cdot 8065$

Statt des zweiten Faktors $1 - 2^n + 2^{2n-1}$ kann man auch

$$1 + 2^n + 2^{n+1} + 2^{n+2} + \ldots + 2^{2(n-1)}$$

schreiben, wonach die Zahlen $1 + 2^2$, $1 + 2^3 + 2^4$, $1 + 2^4 + 2^5 + 2^6$, $1 + 2^5 + 2^6 + 2^7 + 2^8$ u. s. w. Faktoren der Zahlform $1 + 2^r$ sind.

Das Produkt des Faktors $1 + 2^n$ und der Summe

$$\begin{aligned}
&1 - 1 + 2^n - 2^{2n} + 2^{3n} - \ldots + 2^{(2m-3)n} - 2^{(2m-2)n} + 2^{(2m-1)n} \\
&\quad - 1 + 2^n - 2^{2n} + 2^{3n} - \ldots + 2^{(2m-3)n} - 2^{(2m-2)n} \\
&\quad - 1 + 2^n - 2^{2n} + 2^{3n} - \ldots + 2^{(2m-3)n} \\
&\quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
&\quad - 1 + 2^n - 2^{2n} + 2^{3n} \\
&\quad - 1 + 2^n - 2^{2n} \\
&\quad - 1 + 2^n \\
&\quad - 1
\end{aligned}$$

welche Summe auch

(4) $1 - 2m + (2m - 1)2^n - (2m - 2)2^{2n} + (2m - 3)2^{3n} - \ldots$
$+ 3 \cdot 2^{(2s-3)n} - 2 \cdot 2^{(2s-2)n} + 1 \cdot 2^{(2s-1)n}$

geschrieben werden kann, ist

$$(2^n - 2m) + (1 - 2^n + 2^{2n} - 2^{3n} + \ldots + 2^{2mn})$$

Wenn $2m = 2^n$ oder $m = 2^{n-1}$ genommen wird; so reduzirt sich dieses Produkt auf den zweiten in Klammern geschlossenen Theil. Wird dieser Theil mit $1 + 2^n$ multiplizirt; so ist das Produkt nach Formel (1) gleich $1 + 2^{(2m+1)n}$. Da nun jener Theil selbst schon das Produkt aus $1 + 2^n$ und dem durch (4) dargestellten Faktor ist; so enthält die Zahl $1 + 2^{(2m+1)n}$ für $m = 2^{n-1}$ den Faktor $(1 + 2^n)^2 = 1 + 2^{n+1} + 2^{2n}$, oder man hat hierfür

$$(5)\quad (1 + 2^{n+1} + 2^{2n})\{1 - 2m + (2m-1)2^n - (2m-2)2^{2n} + \ldots + 3 \cdot 2^{(2m-3)n} - 2 \cdot 2^{(2m-2)n} + 1 \cdot 2^{(2m-1)n}\} = 1 + 2^{(2m+1)n}$$

z. B. für $n = 1$, $m = 1$, dann für $n = 2$, $m = 2$, dann für $n = 3$, $m = 4$, dann für $n = 4$, $m = 8$, dann für $n = 5$, $m = 16$

$(1+2^2+2^2)(1-2+2) = 1 + 2^3$

$(1+2^3+2^4)(1-4+3.2^2-2.2^4+1.2^6) = 1 + 2^{10}$

$(1+2^4+2^6)(1-8+7.2^3-6.2^6+5.2^9-\ldots+2^{21}) = 1+2^{27}$

$(1+2^5+2^8)(1-16+15.2^4-14.2^8+13.2^{12}-\ldots+2^{60}) = 1+2^{68}$

$(1+2^6+2^{10})(1-32+31.2^5-30.2^{10}+28.2^{15}-\ldots+2^{155}) = 1+2^{165}$

6) Diese Formeln (1) bis (5) stellen nur Zerlegungen solcher Zahlen von der Form $1 + 2^r$ dar, worin der Exponent einen unpaaren Faktor hat; eine Zerlegung der Zahlen von der allgemeinen Form $1 + 2^{mn}$ ist damit nicht erreicht.

Eine Multiplikation des Trinoms $1 + 2^{4n+1} + 2^{4n+3}$ mit der Reihe $-1 + 2^2 - 2^4 + \ldots + 2^{4m-4n-2}$ giebt das Produkt

$$(-1 + 2^2 - 2^4 + \ldots + 2^{4m-4n-2}) - 2^{4n+1} + 2^{4m+1}$$

Für $m = 1$, $n = 0$ reduzirt sich dasselbe auf $-1 + 2^2 - 2 + 2^3 = 1 + 2^3$, lehrt also, dass $1 + 2 + 2^3 = 11$ ein Faktor von $1 + 2^5$ ist.

Wenn man das Trinom $1 + 2^{4n-1} + 2^{4n+1}$ mit dem Aggregate

$$(1 - 2^2 + 2^4 - \ldots + 2^{4m}) + (-2^{4m+3} + 2^{4m+5} - \ldots + 2^{4m+4n+1})$$

multiplizirt; so erhält man das Produkt

$$(1 - 2^2 + 2^4 - \ldots + 2^{4m}) + (-2^{4m+3} + 2^{4m+5} - \ldots - 2^{4m+4n-1}) + 2^{4n-1} + 2^{4m+8n+2}$$

Der Ausdruck unter der ersten und der unter der zweiten Klammer reduzirt sich auf ein einziges Glied wenn $m = 0$ und $n = 1$ ist, und zugleich erhält das zweite Glied den negativen Werth des dritten. Hierdurch wird das Produkt gleich $1 + 2^{10}$ und lehrt, dass die Zahl $1 + 2^{10}$ den Faktor $1 + 2^3 + 2^5 = 41$ hat.

Multiplizirt man das Trinom $1 + 2^{4n-1} + 2^{4n+1}$ mit dem Aggregate

$$1 - 2^m - 2^{m+2} - 2^{m+7} + (2^{m+8} - 2^{m+10} + 2^{m+12} - \ldots + 2^{m+4n+8})$$

so ergiebt sich das Produkt

$$1 + 2^{m+8n+9} + 2^{4n-1} + 2^{4n+1} - 2^m - 2^{m+2} - 2^{m+7} + (2^{m+8} - 2^{m+10} + \ldots + 2^{m+4n}) - 2^{m+4n-1}$$

Dieses Produkt wird sich auf die ersten beiden Glieder, also auf eine Zahl von der Form $1 + 2^r$ reduziren, wenn die Summe aller übrigen gleich null wird. Diess geschieht, wenn zunächst die in Klammern geschlossene Reihe sich auf ein Glied vereinfacht, also $m + 4n = m + 8$, mithin $n = 2$ wird. Hierdurch wird die zu annullirende Grösse

$$2^7 + 2^9 - 2^m - 2^{m+2}$$

und die zu diesem Zwecke zu erfüllende Bedingung ist $m = 7$. Alsdann wird das obige Produkt gleich $1 + 2^{32} = 1 + 2^{2^5}$ und daraus geht hervor, dass $1 + 2^{32}$ keine Primzahl ist, sondern den Faktor $1 + 2^7 + 2^9 = 641$ hat, während der andere Faktor

$$1 - 2^7 - 2^9 - 2^{14} + 2^{15} - 2^{17} + 2^{19} - 2^{21} + 2^{23}$$
$$= 1 + 2^7 + 2^8 + 2^{10} + 2^{11} + 2^{12} + 2^{13} + 2^{17} + 2^{18} + 2^{21} + 2^{22}$$

ist.

7) Es lassen sich auf diese Weise noch manche anderen Formeln für die Zerlegung der Zahlen $1 + 2^r$ aufstellen. Dabei drängt sich die Frage auf, ob jede beliebige unpaare Zahl q ein Faktor irgend einer Zahl von der Form $1 + 2^r$ sein könne. Um diese Frage zu entscheiden, stellen wir die gegebene Zahl q in der Form $1 + 2^a + 2^b + 2^c + \ldots$ dar (in welche Form bekanntlich jede unpaare Zahl in einziger Weise gebracht werden kann) und schreiben dieselbe als eine nach der Grundzahl 2 geordnete duale Zahl mit den beiden Ziffern 0 und 1, sodass beispielsweise $13 = 2^3 + 2^2 + 2^0$ die duale Form 1101 mit fallenden Potenzen annimmt. Jede Zahl $2^r + 1$ hat nun die duale Form $100\ldots001$, nämlich in erster und letzter Stelle die Ziffer 1 und in allen Zwischenstellen die Ziffer 0; alle diese Zahlen unterscheiden sich also nur durch die Länge der Zwischenreihe von Nullen. Dividirt man nun mit der Zahl q in die duale Zahl $1000\ldots.$ von unbestimmter Stellenzahl nach den bekannten Regeln der Division dekadischer Zahlen, indem man im Quotienten eine Ziffer nach der anderen bildet und sich vorbehält, im Dividend die Schlussstelle alsdann mit einer 1 auszufüllen, wenn dadurch bei dem nächsten Divisionsakte der Rest 0 erzielt werden kann; so wird jeder Rest, welcher sich bei der Subtraktion jedes einzelnen Partialproduktes von dem unmittelbar darüber stehenden Theile des Dividends darstellt, immer kleiner sein als der Divisor q; es wird sich also endlich entweder der Rest $q - 1 = 2^a + 2^b + 2^c + \ldots$ einstellen, oder es wird sich irgend ein davon verschiedener, aber schon vorher dagewesener Rest wiederholen. Kömmt man vor der Wiederholung irgend eines anderen Restes auf den Rest $q - 1$; so geht, indem man jetzt den Dividend mit der Ziffer 1 schliesst, wodurch der Rest den Werth q erlangt, die Division bei dem nächsten Divisionsakte auf, oder es ergiebt sich nun der Rest 0, die gegebene Zahl q ist also ein Divisor einer Zahl $2^r + 1$. Wiederholt sich jedoch, ehe der Rest $q - 1$ aufgetreten ist, ein schon vorher dagewesener Rest; so werden auch alle folgenden Reste periodisch wiederkehren, wie weit man auch die Schlussziffer des Dividends hinausschieben möge; die Division kann also niemals aufgehen, oder es kann keine Zahl von der Form $2^r + 1$ die Zahl q als Faktor enthalten.

Das Kennzeichen der Untheilbarkeit der Zahlform $2^r + 1$ durch eine gegebene unpaare Zahl $q = 1 + 2^a + 2^b + \ldots$ ist daher die Periodizität der bei der Division entstehenden Reste oder die Periodizität der Ziffern im Dividend. Das Kennzeichen der Theilbarkeit dagegen ist das Erscheinen des Restes $q - 1$. Wenn der letztere Fall eintritt, ist übrigens die Zahl q ein Faktor unendlich vieler Zahlen von der Form $2^r + 1$; denn wenn der Rest $q - 1$ erschienen ist und die Division beim nächsten Akte durch Herunterziehen der Schlussziffer 1 des Dividends den Quotienten $2^n + 2^m + \ldots + 1$ liefert; so kann man diese Division als nicht geschlossen betrachten, wenn man jetzt in die letzte Stelle des Dividends ausser der Ziffer 1 noch die Ziffer -1 einführt, also die letzte Null des ungeschlossenen Dividends $= 1 - 1$ setzt. Indem man jetzt die negative Ziffer -1 als die erste Stelle eines negativen Theiles des Dividends von der Form $(-1)\,00\ldots00\,(-1)$ betrachtet und die Division mit q fortsetzt, ergiebt sich ein negativer Theil des Quotienten, welcher dem ersten positiven in der Ziffernfolge ganz gleich, jedoch von niedrigerem Range ist; der aus diesen beiden Theilen bestehende Abschnitt des Quotienten wird nämlich $(2^n + 2^m + \ldots + 1)\,2^r - (2^n + 2^m + \ldots + 1)$. Am Ende dieses negativen Theiles schliesst die Division bei der Herabziehung der Ziffer -1, d. h. q erscheint als ein Theiler der Zahl $2^{2r} - 1$. Betrachtet man aber die Division nicht als geschlossen, setzt vielmehr in die letzte Stelle des Dividends ausser der Ziffer -1 noch die Ziffer 1; so bildet sich ein dritter und zwar positiver Theil des Quotienten, welcher mit dem ersten identisch ist und lehrt, dass q auch ein Theiler der Zahl $2^{3r} + 1$ ist, indem man den Quotienten $(2^n + \ldots + 1)\,2^{2r} - (2^n + \ldots + 1)\,2^r + (2^n + \ldots + 1) = (2^n + \ldots + 1)\,(2^{2r} - 2^r + 1)$ erhält. Überhaupt erscheint q als ein Theiler jeder Zahl von der Form $2^{(2s+1)r} + 1$ und jeder Zahl von der Form $2^{2sr} - 1$, was auch aus anderen Gründen einleuchtet.

Es ist oftmals bequemer, die duale Division durch eine duale Multiplikation zu ersetzen. Zu dem Zwecke nehmen wir die Zahlen der natürlichen dekadischen Zahlenreihe

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 ...

worin wir zur Abkürzung nur die je zehnte Zahl vollständig, die Zwischenzahlen aber nur mit einer einzigen Ziffer folgendermaassen schreiben

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 ...

als die Exponenten der Grundzahl 2, erblicken also in dieser Reihe die Vertreter der Grössen 2^0, 2^1, 2^2, 2^3 u. s. w. Die Einschliessung einer Zahl in dieser Reihe in Parenthesen zeigt an, dass die betreffende Potenz von 2 fehlt oder dass an dieser Stelle der mit steigenden Potenzen geschriebenen dualen Zahl eine 0 steht, während jede nicht eingeklammerte Zahl eine 1 in der dualen Zahl vertritt. So ist z. B. die dekadische Zahl 13 gleich der dualen 0 (1) 2 3 und die Zahl $1 + 2^5$ ist durch 0 (1) (2) (3) (4) 5 dargestellt.

Die Multiplikation eines dualen Multiplikand mit einem dualen Multiplikator vollzieht sich nun in der Weise, dass man den Multiplikand für jede gültige Stelle des Multiplikators niederschreibt, indem man denselben

immer an derjenigen Stelle beginnt, welche einer seiner gültigen Stellen entspricht. Alsdann zählt man in jeder Vertikalreihe die darin stehenden gültigen Stellen, und, indem man beachtet, dass je zwei solche Stellen eine gültige Stelle der nächsten Vertikalreihe ausmachen, überträgt man bei einer paaren Stellenzahl die Hälfte und bei einer unpaaren Stellenzahl die Hälfte der um eine verminderten Stellenzahl in die nächste Vertikalreihe. So ergiebt z. B. die Multiplikation der Zahl 89 = 0 (1) (2) 3 4 (5) 6 mit der Zahl 13 = 0 (1) 2 3 folgende Rechnung

0	(1)	(2)	3	4	(5)	6					
		0	(1)	(2)	3	4	(5)	6			
			0	(1)	(2)	3	4	(5)	6		
				$\widehat{1}$	$\widehat{1}$	$\widehat{1}$	$\widehat{2}$	$\widehat{1}$	$\widehat{1}$	$\widehat{1}$	
1	.	1	.	.	.	.	1	.	.	1	
oder 0	(1)	2	(3)	(4)	(5)	(6)	7	(8)	(9)	10	

d. h. es ist $(2^0 + 2^3 + 2^4 + 2^6)\ (2^0 + 2^2 + 2^3) = 2^0 + 2^2 + 2^7 + 2^{10}$.

Wenn es nun darauf ankömmt, den Quotienten der Division eines gegebenen Divisors in einen gegebenen Dividend zu ermitteln; so kennt man, indem der gegebene Divisor mit dem vorstehenden Multiplikator und der gegebene Dividend mit dem Produkte, der gesuchte Quotient aber mit dem Multiplikand identifizirt wird, in der vorstehenden Rechnung die Anfangsstellen für den sich wiederholenden Multiplikand und alle gültigen Stellen des Produktes und hat nur zu ermitteln, welche Stellen des Multiplikand einzuklammern sind, damit das gegebene Produkt herauskömmt. Zu dem Ende sieht man nach, ob in der ersten Vertikalreihe die oberste Stelle stehen bleiben oder eingeklammert werden muss: ist sie einzuklammern; so muss sie in allen Horizontalreihen eingeklammert werden. Darauf geht man zur zweiten, dritten u. s. w. Vertikalreihe über, indem man unter Berücksichtigung der Überträge nachsieht, ob die oberste Stelle einzuklammern ist oder nicht, in welchem ersteren Falle dieselbe Stelle in jeder Horizontalreihe einzuklammern ist.

Für unseren speziellen Zweck kömmt es nur darauf an, Faktoren einer dualen Zahl von der Form 100 ... 001 zu ermitteln, sodass also in jeder Vertikalreihe eine paare Anzahl gültiger Stellen erscheinen muss, mit Ausnahme der ersten und letzten Vertikalreihe, welche je eine gültige Stelle enthalten muss. Der gegebene Multiplikator ist also dann ein Faktor der gedachten Zahlform, wenn es sich bei dem vorstehenden Verfahren ereignet, dass von irgend einer Vertikalreihe an, in welche aus der vorhergehenden Vertikalreihe eine einzige Einheit zu übertragen ist, in der untersten Horizontalreihe sämmtliche Stellen bis zu demjenigen Zeiger einschliesslich, welcher der obersten Zahl jener Vertikalreihe vorhergeht, eingeklammert sind. In diesem Falle kann die Operation geschlossen werden, indem das Produkt in der gedachten Vertikalreihe als letzte Ziffer eine 1 erhält. Wenn sich dagegen vor Eintritt dieses Falles im Multiplikand eine Ziffernfolge von der Länge des Multiplikators und der gleiche Übertrag auf die nächste Vertikalreihe wiederholt; so kann sich niemals ein Produkt von der verlangten Form einstellen. Wenn man im ersten Falle die oberste Stelle der letzten Vertikalreihe, welche im Produkte die

Ziffer 1 aufnehmen würde, mit einer gültigen Stelle ausfüllt; so ist die Operation nicht geschlossen, sondern schliesst erst wieder nach einer gewissen Reihe von Gliedern, bestätigt also wie vorhin, dass der Multiplikator ein Theiler unendlich vieler Zahlen von der gegebenen Form ist.

Um z. B. zu ermitteln, ob $13 = 0\ (1)\ 2\ 3$ ein Faktor von $1 + 2^r$ ist, hat man folgende Rechnung

0	(1)	2	(3)	(4)	(5)				
		0	(1)	2	(3)	(4)	(5)		
			0	(1)	2	(3)	(4)	(5)	
			$\widehat{1}$	$\widehat{1}$	$\widehat{1}$	$\widehat{1}$			
1	0	0	0	0	0	1			$= 1 + 2^6$

aus welcher hervorgeht, dass 13 ein Faktor von $1 + 2^6$ ist. Setzt man die Operation über den Zeiger 5 hinaus fort; so ergiebt sich

0	(1)	2	(3)	(4)	(5)	6	7	(8)	9	10	1	(2)	(3)	4	(5)	(6)	(7)	
	0	(1)	2	(3)	(4)	(5)	6	7	(8)	9	10	1	(2)	(3)	4	(5)	(6)	(7)
		0	(1)	2	(3)	(4)	(5)	6	7	(8)	9	10	1	(2)	(3)	4	(5)	(6)	(7)
			$\widehat{1}$	$\widehat{1}$	$\widehat{1}$	$\widehat{1}$	$\widehat{1}$	$\widehat{1}$	$\widehat{1}$	$\widehat{2}$	$\widehat{2}$	$\widehat{2}$	$\widehat{2}$	$\widehat{2}$	$\widehat{2}$	$\widehat{1}$	$\widehat{1}$	$\widehat{1}$	
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

$$= 1 + 2^{18}$$

wonach 13 auch ein Faktor von $1 + 2^{18}$ ist.

8) Auf diese Weise ergiebt sich sofort, wenn man das Binom $1 + 2^n$ zum Multiplikator nimmt, dass

$$(1 + 2^n)\ (1 + 2^n + 2^{n+1} + 2^{n+2} + \ldots + 2^{2n-1}) = 1 + 2^{3n}$$

ist, dass also nicht nur jede Zahl von der Form $1 + 2^n$, sondern auch jede Zahl von der Form $1 + 2^n + 2^{n+1} + \ldots + 2^{2n-1}$, also z. B. die Zahl $1 + 2 = 3$, $1 + 2^2 + 2^3 = 13$, $1 + 2^3 + 2^4 + 2^5 = 57$, $1 + 2^4 + 2^5 + 2^6 + 2^7 = 249$ etc. ein Faktor von $1 + 2^{3n}$ ist.

Ferner ersieht man, dass, wenn man das Trinom $1 + 2^n + 2^{n+1}$ zum Multiplikator nimmt,

$$(1 + 2^n + 2^{n+1})\ (1 + 2^n + 2^{n+2} + 2^{n+3} + 2^{2n+3} + 2^{3n} + 2^{3n+2}) = 1 + 2^{3n+5} + 2^{4n} + 2^{4n+1} + 2^{4n+2} + 2^{4n+3}$$

ist, dass also, wenn $4n = 3n + 5$ oder $n = 5$ ist, das Produkt sich auf $1 + 2^{4n+4}$ reduzirt, dass also $1 + 2^5 + 2^6 = 97$ ein Faktor von $1 + 2^{24}$ ist.

Für das Trinom $1 + 2^n + 2^{n+2}$ als Multiplikator ergiebt sich

$$(1 + 2^n + 2^{n+2})\ (1 + 2^n + 2^{n+1} + 2^{n+3} + 2^{n+4} + 2^{n+5} + \ldots + 2^{2n-1} + 2^{2n+3} + 2^{2n+4} + 2^{3n} + 2^{3n+1}) = 1 + 2^{3n+7} + 2^{4n} + 2^{4n+1} + 2^{4n+2} + 2^{4n+3}$$

Ist nun $4n = 3n + 7$ oder $n = 7$; so wird das Produkt $1 + 2^{4n+4} = 1 + 2^{32}$, woraus folgt, dass $1 + 2^7 + 2^9 = 641$ ein Faktor von $1 + 2^{32}$, mithin $1 + 2^{2^5}$ keine Primzahl ist.

Das Trinom $1 + 2^n + 2^{n+m}$ als Multiplikator liefert

$$(1 + 2^n + 2^{n+m})\ (1 + 2^n + 2^{n+1} + 2^{n+2} + \ldots + 2^{n+m-1})$$
$$= 1 + 2^{n+m+1} + 2^{2n} + 2^{2n+1} + 2^{2n+2} + \ldots + 2^{2n+2m-1}$$

Wird $2n = n + m + 1$ oder $n = m + 1$; so wird

$$(1 + 2^n + 2^{n-1})\ (1 + 2^n + 2^{n+1} + 2^{n+2} + \ldots + 2^{2(n-1)}) = 1 + 2^{2(2n-1)}$$

mithin für $n = 2, 3, 4, 5 \ldots$

$$(1 + 2^2 + 2^3)\ (1 + 2^2) = 1 + 2^6$$
$$(1 + 2^3 + 2^5)\ (1 + 2^3 + 2^4) = 1 + 2^{10}$$
$$(1 + 2^4 + 2^7)\ (1 + 2^1 + 2^5 + 2^6) = 1 + 2^{14}$$
$$(1 + 2^5 + 2^9)\ (1 + 2^5 + 2^6 + 2^7 + 2^8) = 1 + 2^{18}$$

u. s. f.

9) Einige Zahlformen, welche keine Faktoren von $1 + 2^r$ sein können, ergeben sich folgendermaassen. Ein Multiplikator von der Form $1 + 2 + 2^2 + 2^3 + \ldots + 2^n = 2^{n+1} - 1$ (mit Ausnahme von $1 + 2 = 3$) bedingt einen unendlichen periodischen Multiplikand, kann also kein Faktor von $1 + 2^r$ sein. So erhält man z. B. für $1 + 2 + 2^2 = 7$ den dualen Multiplikand 111011011011 ... Hiernach kann keine der Zahlen 7, 15, 31, 63, 127, 255 etc. ein Faktor von $1 + 2^r$ sein. Keine Primzahl von der Form $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$, mit Ausnahme der Zahl 3, wie z. B. 7, 31, 127 u. s. w., ist daher in der Form $1 + 2^r$ enthalten.

Das Nämliche ergiebt sich für die Zahlen von der Form $1 + 2 + 2^2 + 2^4 + 2^8 + \ldots + 2^{2^n}$. Keine dieser Zahlen, mit Ausnahme der Zahl 3, wie z. B. 7, 23, 279, 65815 etc., ist ein Faktor von $1 + 2^r$.

10) Die allgemeinen Bedingungen für die Zerlegbarkeit einer dualen Zahl lassen sich folgendermaassen aufstellen. Eine unpaare Zahl $p = 1 + 2^a + 2^b + \ldots + 2^n$, deren höchstes Glied den Exponenten n hat, ist in der allgemeinen Form

$$p = c_0\, 2^0 + c_1\, 2^1 + c_2\, 2^2 + \ldots + c_n\, 2^n$$

enthalten, worin die Koeffizienten c_0, c_a, c_b ... c_n den Werth 1, alle übrigen aber den Werth 0 haben. Dieselbe kann als das Produkt der beiden Faktoren

$$(v_0\, 2^0 + v_1\, 2^1 + \ldots + v_n\, 2^n)\ \ (w_0\, 2^0 + w_1\, 2^1 + \ldots + w_n\, 2^n)$$

angesehen werden, worin von den Koeffizienten v und w die ersten beiden v_0 und w_0, ausserdem aber noch gewisse andere den Werth 1, alle übrigen aber den Werth 0 haben. Führt man die Multiplikation aus; so erhält man den Ausdruck

$$u_0\, 2^0 + u_1\, 2^1 + u_2\, 2^2 + \ldots + u_{2n}\, 2^{2n}$$

dessen Koeffizienten folgende Werthe haben

$$
\begin{array}{lllllllllll}
u_0 & = v_0 w_0 & & & & & & & & & \\
u_1 & = v_0 w_1 & + v_1 w_0 & & & & & & & & \\
u_2 & = v_0 w_2 & + v_1 w_1 & + v_2 w_0 & & & & & & & \\
u_3 & = v_0 w_3 & + v_1 w_2 & + v_2 w_1 & + v_3 w_0 & & & & & & \\
 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\
u_{n-1} & = v_0 w_{n-1} & + v_1 w_{n-2} & + v_2 w_{n-3} & + \ldots & + v_{n-2} w_1 & + v_{n-1} w_0 & & & & \\
u_n & = v_0 w_n & + v_1 w_{n-1} & + v_2 w_{n-2} & + \ldots & + v_{n-2} w_2 & + v_{n-1} w_1 & + v_n w_0 & & & \\
u_{n+1} & = & v_1 w_n & + v_2 w_{n-1} & + \ldots & + v_{n-2} w_3 & + v_{n-1} w_2 & + v_n w_1 & & & \\
u_{n+2} & = & & v_2 w_n & + \ldots & + v_{n-2} w_4 & + v_{n-1} w_3 & + v_n w_2 & & & \\
 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\
u_{2n-2} & = & & & & v_{n-2} w_n & + v_{n-1} w_{n-1} & + v_n w_{n-2} & & & \\
u_{2n-1} & = & & & & & v_{n-1} w_n & + v_n w_{n-1} & & & \\
u_{2n} & = & & & & & & v_n w_n & & &
\end{array}
$$

Dieses Produkt muss der gegebenen Zahl $c_0 2^0 + c_1 2^1 + c_2 2^2 + \ldots + c_n 2^n$ gleich sein, und, wenn man die in jedem Gliede enthaltenen nächst höheren Einheiten auf die nächst höheren Glieder überträgt, muss der entstehende Ausdruck mit der gegebenen Zahl identisch, d. h. seine Koeffizienten müssen den Koeffizienten $c_0, c_1, c_2 \ldots c_n$ gleich werden. Bezeichnet z_r die Anzahl der Einheiten vom Grade r, welche auf den nächst höheren Grad $r + 1$ zu übertragen sind; so muss, damit in diesem Gliede der Koeffizient c_{r+1} erscheinen kann, $u_{r+1} + z_r$ paar, resp. unpaar sein, jenachdem $c_{r+1} = 0$ oder $= 1$ ist, man muss also

$$u_{r+1} + z_r = 2 z_{r+1} + c_{r+1} \tag{6}$$

haben, indem z_{r+1} den Übertrag auf das folgende Glied bezeichnet. Hierdurch ergiebt sich nachstehende Reihe von Beziehungen

$$
\begin{aligned}
u_1 + z_0 &= 2 z_1 + c_1 \\
u_2 + z_1 &= 2 z_2 + c_2 \\
u_3 + z_2 &= 2 z_3 + c_3 \\
u_4 + z_3 &= 2 z_4 + c_4
\end{aligned}
$$

u. s. w.

Indem man aus den ersten beiden Gleichungen die Grösse z_1, dann mit Hülfe der dritten die Grösse z_2, dann mit Hülfe der vierten die Grösse z_3 u. s. w. eliminirt, ergiebt sich, da $v_0 = w_0 = u_0 = c_0 = 1$ und daher $z_0 = 0$ ist,

$$
\begin{aligned}
& u_1 + 2 u_2 + 4 u_3 + 8 u_4 + \ldots + 2^{r-1} u_r \\
&= 2^r z_r + c_1 + 2 c_2 + 4 c_3 + 8 c_4 + \ldots + 2^{r-1} c_r
\end{aligned}
$$

Diese Gleichung gilt für jeden Werth von r; da aber für $r = n$ $c_n = 1$ und $z_n = 0$ ist und für jeden höheren Werth jedes c und jedes z den Nullwerth annimmt; so erhält man für $r = n$ als erste Bedingung

$$u_1 + 2u_2 + 4u_3 + \ldots + 2^{n-1} u_n = c_1 + 2c_2 + 4c_3 + \ldots + 2^{n-1} c_n \tag{7}$$

für alle höheren Werthe von r aber folgende Gruppe von n Bedingungen

$$u_{n+1} = 0 \quad u_{n+2} = 0 \text{ u. s. w. } u_{2n} = 0 \tag{8}$$

Eine Substitution der Werthe von u giebt, wenn man der Symmetrie wegen die Grössen v_0 und w_0 beibehält, als erste Bedingung die Gleichung

$$(9)\quad \begin{aligned}&(v_0 w_1 + v_1 w_0) + 2\,(v_0 w_2 + v_1 w_1 + v_2 w_0)\\ &+ 4\,(v_0 w_3 + v_1 w_2 + v_2 w_1 + v_3 w_0) + \ldots\\ &+ 2^{n-1}\,(v_0 w_n + v_1 w_{n-1} + \ldots + v_n w_0)\\ &= c_1 + 2c_2 + 4c_3 + \ldots + 2^{n-1} c_n = \frac{1}{2}(p-1)\end{aligned}$$

wofür man auch schreiben kann

$$(10)\quad \begin{aligned}&v_0(w_1 + 2w_2 + 4w_3 + \ldots 2^{n-1}w_n) + v_1(w_0 + 2w_1 + 4w_2 + \ldots + 2^{n-1}w_{n-1})\\ &+ 2\,v_2\,(w_0 + 2\,w_1 + 4\,w_2 + \ldots + 2^{n-2}\,w_{n-2})\\ &+ 4\,v_3\,(w_0 + 2\,w_1 + 4\,w_2 + \ldots + 2^{n-3}\,w_{n-3}) + \ldots\\ &+ 2^{n-2}v_{n-1}(w_0 + 2w_1) + 2^{n-1}v_n w_0 = c_1 + 2c_2 + 4c_3 + \ldots + 2^{n-1}c_n\\ &= \frac{1}{2}(p-1)\end{aligned}$$

Die Gruppe der übrigen n Bedingungen zerfällt, da die Annullirung irgend eines Koeffizienten u die Annullirung jedes seiner Glieder verlangt, in folgende Gleichungen

$$(11)\quad \begin{aligned}0 = v_1 w_n &= v_2 w_{n-1} = \ldots = v_{n-2} w_3 = v_{n-1} w_2 &&= v_n w_1\\ &= v_2 w_n = \ldots = v_{n-2} w_4 = v_{n-1} w_3 &&= v_n w_2\\ &\quad\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &= v_{n-2} w_n = v_{n-1} w_{n-1} &&= v_n w_{n-2}\\ &= v_{n-1} w_n &&= v_n w_{n-1}\\ &&&= v_n w_n\end{aligned}$$

Das ganze System der Bedingungsgleichungen ist für v und w symmetrisch; es können also mit einem Male alle v und w von gleichen Zeigern miteinander vertauscht werden, was einer Vertauschung der beiden Faktoren der gegebenen Zahl entspricht.

Eine Auflösung der Aufgabe bietet sich stets dar, nämlich die, welche sich für $v_0 = 1$, $w_0 = 1$ und $w_1 = w_2 = w_3 = \ldots = w_n = 0$ ergiebt. Hierdurch ist die Gruppe der letzten n Bedingungen erfüllt und die erste Bedingung wird, da $v_0 = 1$ ist,

$$\begin{aligned}v_1 + 2v_2 + 4v_3 + \ldots + 2^{n-1}v_n &= c_1 + 2c_2 + 4c_3 + \ldots + 2^{n-1}c_n\\ &= \frac{1}{2}(p-1)\end{aligned}$$

Diese Gleichung erfordert $v_1 = c_1$, $v_2 = c_2 \ldots v_n = c_n$ und stellt, da $v_0 = c_0 = 1$ ist, die gegebene Zahl p selbst dar, während der andere Faktor gleich 1 ist. Eine zweite Auflösung ergiebt sich durch die Vertauschung der v und w und liefert als ersten Faktor die Einheit und als zweiten die Zahl p.

Hinsichtlich der letzten Gruppe von n Bedingungen; so hat die Annullirung irgend eines v oder w keinen Einfluss auf die übrigen v und w. Setzt man aber irgend ein v, insbesondere $v_r = 1$; so erfordert Diess nothwendig die Annullirung aller r Grössen w_{n-r+1}, w_{n-r+2}, $\ldots$ w_n,

und ebenso erfordert die Annahme $w_r = 1$ die Annullirung aller Grössen $v_{n-r+1}, v_{n-r+2} \ldots v_n$.

Wird daher die Grösse $\frac{1}{2}(p-1)$ mittelst der in Rede stehenden Null- und Einheitswerthe der Grössen v und w unter Erfüllung der letzten Gruppe von n Bedingungen in die durch die erste Bedingung ausgesprochene Form gebracht; so ist die Zahl p, wenn diese Darstellung nur in den erwähnten beiden Weisen (welche die Zerlegung $p \,.\, 1$ und $1 \,.\, p$ ergeben) möglich ist, eine Primzahl, und wenn sie noch auf andere Weise möglich ist, eine zusammengesetzte Zahl.

Offenbar haben die aufgestellten $n+1$ Gleichungen auch dann noch Gültigkeit, wenn für v und w beliebige positive und negative ganze Werthe zugelassen werden. Selbst die Zerfällung der letzten Gruppe (10) von n Bedingungen in die Gleichungen (11) findet statt: denn multiplizirt man die vorletzte mit v_n; so ergiebt sich wegen der letzten Bedingung $v_n^2 w_{n-1} = 0$, also, welchen Werth auch v_n und w_{n-1} haben möge, $v_n w_{n-1} = 0$ und demzufolge auch wegen der vorletzten Bedingung. $v_{n-1} w_n = 0$. Ebenso ergiebt die vorvorletzte Bedingung durch Multiplikation mit v_n $v_n w_{n-2} = 0$ und durch Multiplikation mit w_n $v_{n-2} w_n = 0$, also auch $v_{n-1} w_{n-1} = 0$ u. s. f. Jetzt kann übrigens eine Zahl auf mehr als eine Weise in Dualform dargestellt werden, zwei einander gleiche Dualzahlen brauchen also nicht nothwendig identisch zu sein.

Wenn man in die Gleichungen (6) für u die durch v und w ausgedrückten Werthe substituirt; so erhält man für $v_0 = w_0 = 1$ die Gleichungen

$$
\begin{aligned}
(12)\quad w_1 &= c_1 - v_1 + 2z_1 - z_0 \\
w_2 &= c_2 - v_1 w_1 - v_2 + 2z_2 - z_1 \\
w_3 &= c_3 - v_1 w_2 - v_2 w_1 - v_3 + 2z_3 - z_2 \\
w_4 &= c_4 - v_1 w_3 - v_2 w_2 - v_3 w_1 - v_4 + 2z_4 - z_3 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
w_n &= c_n - v_1 w_{n-1} - v_2 w_{n-2} - v_3 w_{n-3} - \ldots - v_{n-1} w_1 - v_n \\
&\quad + 2z_n - z_{n-1}
\end{aligned}
$$

In der ersten dieser n Gleichungen ist $z_0 = 0$ und in der letzten ist $z_n = 0$; für die übrigen z aber kann man beliebige positive oder negative ganze Zahlen unter dem Vorbehalte einführen, dass dadurch die Bedingungen (11) erfüllt werden und dass die n Gleichungen (12), welche die $n-1$ willkürlichen Grössen $z_1, z_2 \ldots z_{n-1}$ enthalten, unter Berücksichtigung der Bedingungen (11) keine Unmöglichkeit verlangen. Indem man den Werth von w_1 aus der ersten in die zweite, alsdann die Werthe von w_1 und w_2 in die dritte Gleichung u. s. f. substituirt, erhält man Formeln, welche die Koeffizienten w des einen Faktors von p durch die Koeffizienten v des anderen Faktors ausdrücken. Neben diesen n Gleichungen sind aber stets die Bedingungen (11) zu berücksichtigen, welche verlangen, dass für jedes v_r, welches nicht gleich null ist, die r Grössen $w_{n-r+1}, w_{n-r+2} \ldots w_n$ gleich null gesetzt werden. Diese letzteren Bedingungen sind es, welche zu der nothwendigen Ein-

schränkung der Unbestimmtheit der Grössen z führen, gleichviel, ob man die Koeffizienten eines Faktors, oder keines Faktors als gegeben ansieht.

Beispielsweise hat die Zahl $39 = 1 + 2 + 2^2 + 2^5$ die beiden Faktoren $3 = 1 + 2$ und $13 = 1 + 2^2 + 2^3$; es ist also, indem man für v und w, wenn diese Koeffizienten als gegeben angesehen werden, nur die Werthe 0 und 1 zulässt,

c_0	c_1	c_2	c_3	c_4	c_5		v_0	v_1	v_2	v_3	v_4	v_5		w_0	w_1	w_2	w_3	w_4	w_5
= 1	1	1	0	0	1		1	1	0	0	0	0		1	0	1	1	0	0

Sieht man den ersten Faktor oder die v als gegeben, den zweiten Faktor aber oder die w als gesucht an; so erfordern die Bedingungen (11) wegen $v_1 = 1$, dass $w_5 = 0$ sei; die Gleichungen (12) werden also

$$\begin{aligned} w_1 &= 2z_1 \\ w_2 &= 1 - w_1 + 2z_2 - z_1 \\ w_3 &= -w_2 + 2z_3 - z_2 \\ w_4 &= -w_3 + 2z_4 - z_3 \\ 0 &= 1 - w_4 - z_4 \end{aligned}$$

Da die letzte Gleichung durch einen geeigneten Werth von z_4 und die erste durch einen Werth von z_0 offenbar erfüllbar ist; so übersieht man sofort, dass auch alle übrigen Gleichungen erfüllbar sind, dass also $1 + 2$ in der That ein Faktor von 39 ist. Man findet

$$\begin{aligned} w_1 &= -z_1 + 3z_2 - 3z_3 + 3z_4 = 2z_1 \\ w_2 &= 1 - z_2 + 3z_3 - 3z_4 \\ w_3 &= -1 - z_3 + 3z_4 \\ w_4 &= 1 - z_4 \end{aligned}$$

In diesen Gleichungen bleiben die Grössen z_1, z_2, z_3, z_4 vollkommen willkürlich unter der Voraussetzung, dass wegen des doppelten Ausdruckes für w_1

$$z_1 - z_2 + z_3 - z_4 = 0$$

sei. Setzt man z. B. alle $z = 0$; so ergiebt sich $w_0, w_1, w_2, w_3, w_4, w_5 = 1, 0, 1, -1, 1, 0$, also der zweite Faktor gleich $1 + 1 \cdot 2^2 - 1 \cdot 2^3 + 1 \cdot 2^4 = 13$. Setzt man alle $z = 1$; so werden die w resp. $= 1, 2, 0, 1, 0, 0$, also der zweite Faktor gleich $1 + 2 \cdot 2 + 1 \cdot 2^3 = 13$. Setzt man alle $z = 2$; so werden die w resp. $1, 4, -1, 3, -1, 0$, also der zweite Faktor gleich $1 + 4 \cdot 2 - 1 \cdot 2^2 + 3 \cdot 2^3 - 1 \cdot 2^4 = 13$. Setzt man $z_1 = z_2 = 1$, $z_3 = z_4 = 0$; so werden die w resp. $1, 2, 0, -1, 1$, also der zweite Faktor gleich $1 + 2 \cdot 2 - 1 \cdot 2^3 + 1 \cdot 2^4 = 13$. Überhaupt erkennt man durch Einführung der allgemeinen Werthe der w in den Ausdruck des zweiten Faktors, dass derselbe

$$1 + w_1 2 + w_2 2^2 + w_3 2^3 + w_4 2^4 + w_5 2^5 = 13 - 2(z_1 - z_2 + z_3 - z_4)$$

ist, also, wofern nur $z_1 - z_2 + z_3 - z_4 = 0$ ist, stets den Werth 13 annehmen wird.

Die generellen Bedingungen für die Erfüllung der Gleichungen (12) ergeben sich durch die Erwägung, dass jeder von 0 verschiedene Werth

eines der darin enthaltenen v die Annullirung einer ganz bestimmten Anzahl der Grössen w nach den Bedingungen zur Folge hat. Hierdurch verschwinden ebenso viel w aus den n Gleichungen (12) und ermöglichen nun die Elimination aller übrigen w, also die Herstellung einer gewissen Anzahl von Gleichungen, in welchen nur die Grössen z neben den v und c erscheinen. Diese letzten Gleichungen nun sind es, welche die Unbestimmtheit der Grössen z beschränken und von deren Erfüllbarkeit die Möglichkeit der Aufgabe abhängt.

Man kann jede unpaare Zahl in der Form $1 + 2v$, also das Produkt zweier unpaaren Faktoren in der Gleichung

$$p = 1 + 2c = (1 + 2v)(1 + 2w) = 1 + 2(v + w +) 4vw$$

darstellen, was statt Gl. (9) die Beziehung $v + w + 2vw = \frac{1}{2}(p-1)$ giebt. Diese Beziehung enthält den Satz, dass, wenn $\frac{1}{2}(p-1)$ als Aggregat der Summe und des doppelten Produktes zweier ganzen Zahlen v und w darstellbar ist, die Zahl p die beiden Faktoren $1 + 2v$ und $1 + 2w$ hat.

Stellen wir von den beiden Faktoren nur den einen in der Form $1 + 2v$, den anderen aber, sowie auch das Produkt p in der generelleren Form dar; so erfordert die erste der Beziehungen (11), dass $w_n = 0$ sei, und die Gleichungen (12) werden nun

$$\begin{aligned}
w_1 &= c_1 - v + 2z_1 \\
w_2 &= c_2 - vw_1 + 2z_2 - z_1 \\
w_3 &= c_3 - vw_2 + 2z_3 - z_2 \\
w_4 &= c_4 - vw_3 + 2z_4 - z_3 \\
&\cdots\cdots\cdots \\
w_{n-1} &= c_{n-1} - vw_{n-2} + 2z_{n-1} - z_{n-2} \\
w_n &= c_n - vw_{n-1} - z_{n-1}
\end{aligned}$$

oder durch Substitution der Werthe von w in die je folgende Gleichung

$$\begin{aligned}
(13)\quad w_1 &= c_1 - v + 2z_1 \\
w_2 &= c_2 - c_1 v + v^2 - (1 + 2v) z_1 + 2z_2 \\
w_3 &= c_3 - c_2 v + c_1 v^2 - v^3 - (1 + 2v)(z_2 - vz_1) + 2z_3 \\
w_4 &= c_4 - c_3 v + c_2 v^2 - c_1 v^3 + v^4 - (1 + 2v)(z_3 - vz_1 + v^2 z_1) + 2z_4 \\
&\cdots\cdots\cdots\cdots\cdots \\
w_{n-1} &= c_{n-1} - c_{n-2} v + c_{n-3} v^2 - \ldots (-1)^{n-1} v^{n-1} \\
&\quad - (1 + 2v)\{z_{n-2} - vz_{n-3} + v^2 z_{n-4} - \ldots (-1)^{n-3} v^{n-3} z_1\} \\
&\quad + 2z_{n-1} \\
w_n &= 0 = c_n - c_{n-1} v + c_{n-2} v^2 - \ldots (-1)^n v^n \\
&\quad - (1 + 2v)\{z_{n-1} - vz_{n-2} + v^2 z_{n-3} - \ldots (-1)^{n-2} v^{n-2} z_1\}
\end{aligned}$$

Nach der letzten dieser Gleichungen muss

$$(14) \qquad z_1 v^{n-2} - z_2 v^{n-3} + z_3 v^{n-4} - \ldots (-1)^n z_{n-1} = \frac{v^n - c_1 v^{n-1} + c_2 v^{n-2} - \ldots (-1)^n c_n}{2v+1}$$

sein, und hieraus folgt der Satz: wenn es eine Zahl v giebt, für welche $v^n - c_1 v^{n-1} + c_2 v^{n-2} - \ldots (-1)^n c_n$ durch $2v+1$ theilbar ist; so hat die Zahl p einen Theiler, welcher $= 2v+1$ ist; die Gl. (14) bestimmt den Werth von z_{n-1} durch die Grössen $z_1, z_2, z_3 \ldots z_{n-2}$, welche sämmtlich willkürlich bleiben, also auch $= 0$ gesetzt werden können, und durch ihre Substitution in die Gleichungen (13) die Werthe des Koeffizienten w des zweiten Faktors von p ergeben. Zwei Werthe von v giebt es immer, welche diese Bedingung erfüllen: der erste ist der Werth $v = 0$, welcher den Faktor $2v+1 = 1$ ergiebt; der andere Werth ist $v = \frac{1}{2}(p-1) = c_1 + 2c_2 + 4c_3 + \ldots + 2^{n-1} c_n$, welcher den Faktor $2v+1 = p$ ergiebt.

Wenn man den Zähler auf der rechten Seite von Gl. (14) mit 2^n multiplizirt; so wird derselbe

$$\begin{aligned}&(2v)^n - 2c_1 (2v)^{n-1} + 2^2 c_2 (2v)^{n-2} - \ldots (-1)^n 2^n c_n \\ &= (2v+1)\{(2v)^{n-1} - (1+2c_1)(2v)^{n-2} + (1+2c_1+2^2c_2)(2v)^{n-3} - \ldots \\ &\qquad (-1)^{n-1}(1+2c_1+2^2c_2+\ldots+2^{n-1}c_{n-1})\} \\ &\qquad + (-1)^n (1+2c_1+2^2c_2+\ldots+2^n c_n)\end{aligned}$$

Da nun 2^n nur den Primfaktor 2 enthält, also mit der unpaaren Zahl $2v+1$ keinen Faktor gemein haben kann; so muss auch der mit 2^n multiplizirte Zähler in Gl. (14) durch $2v+1$ theilbar sein, und Diess erfordert nach der letzten Umformung die Theilbarkeit der Zahl $1 + 2c_1 + 2^2 c_2 + \ldots + 2^n c_n = p$ durch $2v+1$.

Hieraus ergiebt sich, dass die Theilbarkeit oder Untheilbarkeit der Zahl p gleichbedeutend ist mit der Existenz, resp. Nichtexistenz einer durch $2v+1$ theilbaren Zahl von der Form $v^n - c_1 v^{n-1} + c_2 v^{n-2} - \ldots (-1)^n c_n$. Da man von den beiden Faktoren von p nur den kleineren, welcher $\leqq \sqrt{p}$ ist, in Betracht zu ziehen braucht, für diesen aber $v \leqq \frac{1}{2}(\sqrt{p} - 1)$ ist; so ist $p = 1 + 2c_1 + 2^2 c_2 + \ldots + 2^n c_n$ eine Primzahl, wenn sich unter den Zahlen, welche $\leqq \frac{1}{2}(\sqrt{p} - 1)$ sind, ausser der Zahl 1 keine Zahl v findet, für welche

$$v^n - c_1 v^{n-1} + c_2 v^{n-2} - \ldots (-1)^n c_n$$

durch $2v+1$ theilbar ist, und andererseits lässt p so viel verschiedene Zerlegungen in zwei Faktoren zu, als es verschiedene Zahlen v von der gedachten Beschaffenheit giebt. Wenn $2v+1$ eine zusammengesetzte Zahl ist; so ist jeder Faktor von ihr ein Faktor von p, es giebt also noch einen kleineren Theiler als $2v+1$: fasst man daher die Primfaktoren von p ins Auge; so kann man sagen, dass p eine Primzahl sei,

wenn es unter den Primzahlen von der Form $2v + 1$, welche $\leqq \sqrt{p}$ sind, keine giebt, die in

$$v^n - c_1 v^{n-1} + c_2 v^{n-2} - \ldots (-1)^n c_n$$

aufgeht.

Die Umkehrung dieses Satzes lautet: jenachdem p theilbar oder untheilbar ist, giebt es eine oder keine Zahl von der Form $v^n - c_1 v^{n-1} + \ldots (-1)^n c_n$, welche durch $2v + 1$ theilbar ist.

So findet man z. B. für $p = 15 = 1 + 1.2 + 1.2^2 + 1.2^3$, also $v \leqq \frac{1}{2}(\sqrt{15} - 1) \leqq 1$, dass $v^3 - v^2 + v - 1$ für $v = 0$ durch 1 und für $v = 1$ durch 3 theilbar ist, dass man also nur $15 = 1.15$ und $= 3.5$ hat.

Für $p = 11 = 1 + 1.2 + 0.2^2 + 1.2^3$, also $v \leqq 1$, ist $v^3 - v^2 - 1$ nur für $v = 0$ durch 1 theilbar, 11 ist also eine Primzahl.

11) Der vorstehende Satz ist einer Verallgemeinerung fähig. Setzt man den Faktor von p allgemein gleich $2^m v + 1$; so muss auch $v^r p$ durch $2^m v + 1$ theilbar sein, und umgekehrt, wenn $v^r p$ durch $2^m v + 1$ theilbar ist, wird auch p dadurch theilbar sein. Jetzt schreiben wir

$$v^r p = 2^{n-rm} 2^{rm} c_n v^r + A_1$$

sodass $A_1 = 2^{n-1} c_{n-1} v^r + 2^{n-2} c_{n-2} v^r + \ldots + 2 c_1 v^r + v^r$ ist. Führt man die Division mit $2^m v + 1$ in diesen Ausdruck von $v^r p$ aus, indem man immer mit dem ersten Gliede des Divisors in das erste Glied des Restes dividirt, die Grösse A_1 aber immer als Rest zurückstellt; so ergiebt sich nach s_1-maliger Division der Rest

$$R_1 = (-1)^{s_1} 2^{n-s_1 m} c_n v^{r-s_1} + A_1$$

Jetzt substituiren wir für A_1 seinen Werth, schreiben denselben aber

$$A_1 = 2^{n-1-rm} 2^{rm} c_{n-1} v^r + A_2$$

worin $A_2 = 2^{n-2} c_{n-2} v^r + 2^{n-3} c_{n-3} v^r + \ldots + 2 c_1 v^r + v^r$ ist, indem wir immer in das erste Glied der Grösse A_1 oder ihres Restes dividiren und alle übrigen Glieder des Dividends als Rest zurückstellen; so ergiebt sich nach s_2-maliger Division der Rest

$$R_2 = (-1)^{s_1} 2^{n-s_1 m} c_n v^{r-s_1} + (-1)^{s_2} 2^{n-1-s_2 m} c_{n-1} v^{r-s_2} + A_2$$

In dieser Weise kann man nach Einführung des Werthes von A_2 in der Form

$$A_2 = 2^{n-2-rm} 2^{rm} c_{n-2} v^r + A_3$$

die Division fortsetzen und schliesslich den Rest

$$R = (-1)^{s_1} 2^{n-s_1 m} c_n v^{r-s_1} + (-1)^{s_2} 2^{n-1-s_2 m} c_{n-1} v^{r-s_2} + \ldots$$
$$+ (-1)^t 2^{x+1-tm} c_{x+1} v^{r-t} + v^r (2^x c_x + 2^{x-1} c_{x-1} + \ldots + 2 c_1 + 1)$$

herstellen. Die Grössen r, s_1, $s_2 \ldots t$, x sind willkürlich, müssen jedoch von der Art sein, dass kein Exponent negativ wird. Setzt man alle s und t gleich r; so verschwindet v aus allen Gliedern, welche den ersten

Theil von R bilden. Setzt man ausserdem $x + 1 - r\,m = 0$, also $x = r\,m - 1$; so erniedrigt man den zweiten in v^r multiplizirten Theil auf den kleinstmöglichen Betrag und erhält

$$(15)\quad R = (-1)^r (2^{n-rm} c_n + 2^{n-rm-1} c_{n-1} + 2^{n-rm-2} c_{n-2} + \ldots + c_{rm}) + v^r (2^{rm-1} c_{rm-1} + 2^{rm-2} c_{rm-2} + 2^{rm-3} c_{rm-3} + \ldots + 2c_1 + 1)$$

Bringt man diesen Rest in die Form

$$(16)\quad R = \frac{(-1)^r}{2^{rm}} (2^n c_n + 2^{n-1} c_{n-1} + \ldots + 2^{rm} c_{rm}) + v^r (2^{rm-1} c_{rm-1} + 2^{rm-2} c_{rm-2} + \ldots + 2c_1 + 1)$$

so erscheinen die beiden in Klammern geschlossenen Polynome als zwei Theile der Grösse p, welche entstehen, sobald man die Reihe $2^n c_n + 2^{n-1} c_{n-1} + \ldots + 2c_1 + 1$ an irgend einer Stelle zerschneidet, wo der Zeiger des letzten Gliedes des ersten Theiles ein beliebiges Vielfaches von m ist. Sind A und B zwei solche Theile von p; so ist

$$(17)\quad R = (-1)^r \frac{A}{2^{rm}} + v^r B$$

Hierdurch sind wir zu dem Zahlengesetze gelangt: jenachdem es eine durch $2^m v + 1$ theilbare Zahl von der Form R giebt oder nicht, ist p theilbar oder untheilbar, und umgekehrt, jenachdem p theilbar oder untheilbar ist, giebt es eine durch $2^m v + 1$ theilbare Zahl von der Form R, oder nicht.

In der Formel (17) sind r und m zwei Zahlen, welche unterhalb gewisser Grenzen ganz willkürlich bleiben. Ist nämlich w eine unpaare Zahl und $1 + 2^{m'} w$ ein Faktor von p; so ist auch für jeden Exponenten m, welcher $\leqq m'$ ist, $1 + 2^m (2^{m'-m} w)$ ein Faktor von p, d. h. v kann in dem Ausdrucke $1 + 2^m v$ jeden Werth $2^{m'-m} w$ und m jeden Werth $\leqq m'$ annehmen (wobei jedoch der Werth $m = 0$ unberücksichtigt bleiben kann). Der Exponent r ist dann nur an die Bedingung gebunden, dass $r\,m \leqq n$ sei. Hiernach kann man unter der ausdrücklichen Voraussetzung, dass w eine unpaare Zahl sei,

$$(18)\quad R = (-1)^r \frac{A}{2^{rm}} + (2^{m'-m} w)^r B$$

setzen und behaupten, dass, wenn $1 + 2^{m'} w$ ein Faktor von p ist, jede beliebige Zahl von der Form R, worin r und m willkürlich und nur an die Bedingungen $m \leqq m'$ und $r\,m \leqq n$ gebunden bleiben, durch jenen Faktor theilbar ist, und dass, wenn irgend eine Zahl von dieser Form durch einen solchen Faktor theilbar ist, sie es sämmtlich sind, dass also für eine Primzahl p keine der fraglichen Zahlformen durch den gedachten Faktor theilbar sein kann.

Beispielsweise hat $p = 63 = 2^5 + 2^4 + 2^3 + 2^2 + 2 + 1$ die beiden Faktoren 7 und 9. Für den Faktor $7 = 2 \cdot 3 + 1$ ist

$w = 3$ und $m' = 1$; es kömmt also nur der Werth $v = 3$, $m = 1$ in Betracht: r bleibt willkürlich, es darf jedoch $r\,m$ den Betrag $n = 5$ nicht übersteigen. Für $v = 3$, $m = 1$ ergiebt sich

$$r = 1 \quad R = -\frac{2^5+2^4+2^3+2^2+2}{2} + 3\,.\,1 \quad = -28 = -4\,.\,7$$

$$r = 2 \quad R = \frac{2^5+2^4+2^3+2^2}{2^2} + 3^2\,(2+1) \quad = 42 = 6\,.\,7$$

$$r = 3 \quad R = -\frac{2^5+2^4+2^3}{2^3} + 3^3\,(2^2+2+1) = 182 = 26\,.\,7$$

$$r = 4 \quad R = \frac{2^5+2^4}{2^4} + 3^4\,(2^3+2^2+2+1) = 1218 = 174\,.\,7$$

$$r = 5 \quad R = -\frac{2^5}{2^5} + 3^5\,(2^4+2^3+2^2+2+1) = 7532 = 1076\,.\,7$$

Für den Faktor $9 = 2^3\,.\,1 + 1$ ist $w = 1$ und $m' = 3$; man kann also nach Belieben $v = 1$, $m = 3$ oder $v = 2$, $m = 2$ oder $v = 4$, $m = 1$ setzen. Nimmt man $v = 1$, $m = 3$; so kömmt

$$r = 1 \quad R = -\frac{2^5+2^4+2^3}{2^3} + 1\,(2^2+2+1) = 0 = 0\,.\,9$$

Nimmt man $v = 2$, $m = 2$; so kömmt

$$r = 1 \quad R = -\frac{2^5+2^4+2^3+2^2}{2^2} + 2\,(2+1) = -9 = -1\,.\,9$$

$$r = 2 \quad R = \frac{2^5+2^4}{2^4} + 2^2\,(2^3+2^2+2+1) = 63 = 7\,.\,9$$

Nimmt man $v = 4$, $m = 1$; so kömmt

$$r = 1 \quad R = -\frac{2^5+2^4+2^3+2^2+2}{2} + 4\,.\,1 \quad = -27 = -3\,.\,9$$

$$r = 2 \quad R = \frac{2^5+2^4+2^3+2^2}{2^2} + 4^2\,(2+1) \quad = 63 = 7\,.\,9$$

$$r = 3 \quad R = -\frac{2^5+2^4+2^3}{2^3} + 4^3\,(2^2+2+1) = 441 = 49\,.\,9$$

$$r = 4 \quad R = \frac{2^5+2^4}{2^4} + 4^4\,(2^3+2^2+2+1) = 3843 = 427\,.\,9$$

Will man den vorstehenden Satz benutzen, um nach den Faktoren von p zu forschen; so ist für den kleineren der beiden Faktoren $2^m v + 1 \leqq \sqrt{p}$, also, jenachdem n paar $= 2n'$ oder unpaar $= 2n' + 1$ ist, $2^m v + 1 \leqq 2^{n'} c'_{n'} + 2^{n'-1} c'_{n'-1} + \ldots + 2c' + 1$, mithin

$$v \leqq 2^{n'-m} c''_{n'-m} + 2^{n'-m-1} c''_{n'-m-1} + \ldots + 2c'' + 1$$

und hierin muss stets $m \leqq n'$ sein. Übrigens kann man nach Obigem alle paaren Werthe von v ausschliessen.

Ist U der Quotient $\frac{R}{2^m v + 1}$, also

$$(-1)^r \frac{A}{2^{rm}} + v^r B = U(2^m v + 1)$$

so ist

$$v(2^m U - v^{r-1} B) = (-1)^r \frac{A}{2^{rm}} - U \tag{19}$$

worin U einen beliebigen ganzen Werth haben kann.

Der zweite Faktor von p ist

$$\frac{p}{2^m v + 1} = \frac{Q + U}{v^r}$$

worin Q den Quotienten vertritt, welcher sich bei der obigen Division mit $2^m v + 1$ in $v^r p$ an der Stelle ergiebt, an welcher sich der Rest R aus Gl. (16) einstellt. Für diesen Quotienten findet man

$$\begin{aligned}(20)\quad Q = {} & (2^{n-m} v^{r-1} - 2^{n-2m} v^{r-2} + 2^{n-3m} v^{r-3} - \ldots (-1)^{r+1} 2^{n-rm}) c_n \\ & + (2^{n-1-m} v^{r-1} - 2^{n-1-2m} v^{r-2} + 2^{n-1-3m} v^{r-3} - \ldots (-1)^{r+1} 2^{n-1-rm}) c_{n-1} \\ & + (2^{n-2-m} v^{r-1} - 2^{n-2-2m} v^{r-2} + 2^{n-2-3m} v^{r-3} - \ldots (-1)^{r+1} 2^{n-2-rm}) c_{n-2} \\ & + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & + (2^{(r-1)m} v^{r-1} - 2^{(r-2)m} v^{r-2} + 2^{(r-3)m} v^{r-3} - \ldots (-1)^{r+1}) c_{rm} \\ = {} & (2^{n-rm} c_n + 2^{n-rm-1} c_{n-1} + 2^{n-rm-2} c_{n-2} + \ldots + c_{rm}) \{2^{(r-1)m} v^{r-1} \\ & - 2^{(r-2)m} v^{r-2} + 2^{(r-3)m} v^{r-3} - \ldots (-1)^{r+1}\} \\ = {} & \frac{A}{2^{rm}} \{2^{(r-1)m} v^{r-1} - 2^{(r-2)m} v^{r-2} + 2^{(r-3)m} v^{r-3} - \ldots (-1)^{r+1}\}\end{aligned}$$

worin A denselben Werth hat wie in Gl. (17). Vermöge dieses Quotienten hat man

$$U = \frac{v^r p}{2^m v + 1} - Q$$

und da das erste Glied von U durch v^r theilbar ist; so folgt aus Gl. (19), dass v auch ein Faktor von

$$(-1)^r \frac{A}{2^{rm}} + Q$$

sein muss, was sich durch Gl. (20) unmittelbar bestätigt.

12) Wir beschränken die fernere Untersuchung auf die Zahlform $p = 2^n + 1$, für welche $c_n = 1$ und alle übrigen c gleich null sind, ausserdem beschäftigen wir uns vornehmlich mit dem Falle, wo der Exponent n eine Potenz von 2 ist, und schicken folgende allgemeinen Sätze voraus.

Aus der Beziehung

$$2^{2^\alpha} - 1 = (2^{2^{\alpha-1}} + 1)(2^{2^{\alpha-1}} - 1) = (2^{2^{\alpha-1}} + 1)(2^{2^{\alpha-2}} + 1)(2^{2^{\alpha-3}} - 1) \ldots$$

ergiebt sich

$$2^{2^\alpha} - 1 = (2^{2^{\alpha-1}} + 1)(2^{2^{\alpha-2}} + 1)(2^{2^{\alpha-3}} + 1) \ldots$$
$$(2^{2^3} + 1)(2^{2^2} + 1)(2^{2^1} + 1)(2 + 1)$$
$$= 3 \cdot 5 \cdot 17 \cdot 257 \cdot 513 \ldots (2^{2^{\alpha-1}} + 1)$$

folglich $2^{2^\alpha} = 1 + 3 \cdot 5 \cdot 17 \cdot 257 \cdot 513 \ldots (2^{2^{\alpha-1}} + 1)$ und

$$(21) \quad 2^{2^\alpha} + 1 = 2 + 3 \cdot 5 \cdot 17 \cdot 257 \ldots (2^{2^{\alpha-1}} + 1)$$

In dem zweiten Gliede auf der rechten Seite ist jede Zahl von der Form $2^{2^r} + 1$ bis zur Höhe der Zahl $2^{2^{\alpha-1}} + 1$ enthalten. Da nun das erste Glied gleich 2, also durch keine dieser letzteren Zahlen theilbar ist; so erkennt man, dass keine zwei Zahlen von der Form $2^{2^r} + 1$ ein gemeinschaftliches Maass haben können. Die verschiedenen zusammengesetzten Zahlen von der Form $2^{2^r} + 1$ bestehen daher aus lauter verschiedenen Primfaktoren.

Ausserdem lehrt diese Formel, dass, wenn irgend eine Zahl $2^{2^r} + 1$ zum Model genommen wird, jede höhere Zahl von dieser Form den Rest 2 liefert, oder dass

$$2^{2^n} + 1 \equiv 2 \ mod \ (2^{2^r} + 1)$$

ist.

Da $2^n - 1 = 1 + 2 + 2^2 + 2^3 + \ldots 2^{n-1}$ ist; so hat man auch die Beziehung

$$(22) \quad 3 \cdot 5 \cdot 17 \ldots (2^{2^{\alpha-1}} + 1) = 1 + 2 + 2^2 + 2^3 + \ldots + 2^{2^\alpha - 1}$$

Für den Fall, wo auch α eine Potenz von 2, also nach Vorstehendem

$$2^\alpha - 1 = 3 \cdot 5 \cdot 17 \ldots (2^{\frac{\alpha}{2}} + 1)$$

ist, hat man

$$3 \cdot 5 \cdot 17 \ldots (2^{2^{\alpha-1}} + 1) = 1 + 2 + 2^2 + 2^3 + \ldots + 2^{3 \cdot 5 \cdot 17 \ldots (2^{\frac{\alpha}{2}} + 1)} = 2^{2^\alpha} - 1$$

z. B. für $\alpha = 4$

$$3 \cdot 5 \cdot 17 \cdot 257 = 1 + 2 + 2^2 + \ldots + 2^{3 \cdot 5} = 2^{16} - 1$$

Durch Zusammenfassung je zweier Glieder auf der rechten Seite von Gl. (21) und Division derselben durch 3 findet man für jeden Werth von α

$$5 \cdot 17 \ldots (2^{2^{\alpha-1}} + 1) = 1 + 2^2 + 2^4 + 2^6 + \ldots + 2^{2^\alpha - 2}$$

ebenso durch abermalige paarweise Zusammenfassung der Glieder und Division durch 5

$$17 \cdot 257 \ldots (2^{2^{\alpha-1}} + 1) = 1 + 2^4 + 2^8 + 2^{12} + \ldots + 2^{2^\alpha - 4}$$

und allgemein

$$(23) \quad (2^{2^n} + 1)(2^{2^{n+1}} + 1) \ldots (2^{2^{\alpha-1}} + 1)$$
$$= 1 + 2^{2^n} + 2^{2 \cdot 2^n} + 2^{3 \cdot 2^n} + \ldots + 2^{2^\alpha - 2^n}$$

sowie auch

$$(24)\quad 2^{2^\alpha} + 1 = 2 + 3.5.17 \ldots (2^{2^{n-1}} + 1)(1 + 2^{2^n} + 2^{2\cdot 2^n} + 2^{3\cdot 2^n} + \ldots + 2^{2^\alpha - 2^n})$$

Man kann leicht zeigen, dass keine Zahl von der Form $1 + 2^r$ ein Faktor einer Zahl von der Form $1 + 2^n$ sein kann (welche Werthe r und n auch haben mögen). Denn immer kann der zweite Faktor von $1 + 2^n$ in die Form $1 + 2^m v$ gebracht werden, worin v eine unpaare Zahl ist. Nun kann aber nicht

$$1 + 2^n = (1 + 2^r)(1 + 2^m v) = 1 + 2^r + 2^m v + 2^{r+m} v$$

oder $$2^n = 2^r + 2^m v + 2^{r+m} v$$

sein: denn, da sowohl r, als auch $m < n$ sind; so müsste, wenn $r < m$ wäre, $2^{n-r} = 1 + 2^{m-r} v + 2^m v$ und, wenn $r > m$ wäre, $2^{n-m} = 2^{r-m} + v + 2^r v$ sein, wovon weder das Eine, noch (wegen des unpaaren v) das Andere möglich ist.

13) Wenden wir jetzt den Satz aus Nr. 11 auf den Fall an, wo die zu zerlegende Zahl p die Form $2^n + 1$ hat und $n = 2^\alpha$ eine Potenz von 2 ist; so wird wegen $c_n = 1$ und $c_{n-1} = c_{n-2} = \ldots = c_1 = 0$ in Gl. (17) $A = 2^n$, $B = 1$ folglich

$$R = (-1)^r 2^{n-rm} + v^r$$

Die Zahl p wird also eine zusammengesetzte sein oder nicht, wenn es einen Werth von v giebt, durch welchen dieser Ausdruck von R für irgend welche Werthe von r und m durch $1 + 2^m v$ theilbar wird. Könnte der Rest R dem Faktor $1 + 2^m v$ gleich werden; so müsste nach Gl. (19) v ein Faktor von $(-1)^r 2^{n-rm} - 1$ sein.

Nimmt man beispielsweise $n = 2^5 = 32$; so kann man, da r und m innerhalb gewisser Grenzen willkürlich sind, die Exponenten in dem Ausdrucke R dadurch möglichst erniedrigen, dass man einmal $r = 4$ und $m = 7$ setzt, weil dadurch $32 - rm = 4$ und $R = 2^4 + v^4$ wird. Den Nullwerth kann R und daher auch U nicht annehmen, weil sonst v nach Gl. (19) ein Faktor von 2^{n-rm} sein müsste, was nach dem Schlusse von Nr. 12 nicht möglich ist. Könnte $R = 1 + 2^7 v$ oder $U = 1$ werden; so müsste v ein Faktor von $2^4 - 1 = 15$, also gleich 3, 5 oder 15 sein. Man findet, dass $v = 5$ der Bedingung genügt, indem $2^4 + 5^4 = 641$ durch $1 + 2^7 5 = 641$ theilbar ist. Hätte man $r = 5$, $m = 6$ genommen; so müsste $1 + 2^6 v$ ein Faktor von $-2^2 + v^5$ sein. In der That, erweis't sich für $v = 10$ die Zahl $1 + 2^6 . 10 = 641$ als ein Faktor von $-2^2 + 10^5 = 99996$. Da der unpaare Werth $v = 5$ für $m = 7$ der Forderung genügt; so ist klar, dass jede Zahl von der Form $(-1)^r 2^{32-rm} + v^r$, welchen Werth von $m \leqq 7$ und welchen Werth von r, wodurch $rm < 32$ bleibt, man auch annehmen möge, durch $1 + 2^7 5 = 641$ theilbar ist, sobald für v der geeignete Werth substituirt wird, der nur zwischen den Werthen 5, 10, 20, 40, 80, 160, 320, 640 variiren wird. Die vorstehende Rechnung liefert wiederum das bekannte Resultat, dass $2^{32} + 1$ keine Primzahl ist, sondern den Faktor 641 hat. Der zweite Faktor hat nach Nr. 11 die Form

$$\frac{Q+U}{v^r} = \frac{1}{v^r}\left\{\begin{array}{c} 2^{n-m}v^{r-1} - 2^{n-2m}v^{r-2} + 2^{n-3m}v^{r-3} - \ldots \\ (-1)^{r+1}2^{n-rm} + U \end{array}\right\}$$
$$= \frac{1}{5^4}\,(2^{35}5^3 - 2^{18}5^2 + 2^{11}5 - 2^4 + 1)$$

und ist $6\,700\,417 = 1 + 2^7 . 52347 = 1 + 2^7 . 3 . 17449$, der Werth $v = 52347$ würde daher der obigen Bedingung ebenso gut entsprechen wie der Werth $v = 5$.

14) Den kürzesten Weg zur Zerlegung einer Zahl in ihre Faktoren und, eventuell, zur Erkenntniss ihrer Eigenschaft als Primzahl bietet die nachstehende Behandlung der in Nr. 10 aufgestellten Gleichungen dar. Wir setzen also die zu zerlegende Zahl

$$p = c_0 + c_1 2 + c_2 2^2 + \ldots - c_n 2^n$$

ihre Faktoren jedoch

$$q_1 = v_0 + v_1 2 + v_2 2^2 + \ldots + v_x 2^x$$
$$q_2 = w_0 + w_1 2 + w_2 2^2 + \ldots + w_y 2^y$$

und das aus der Multiplikation der letzteren sich ergebende Produkt $q_1 q_2$, welches $= p$ sein soll,

$$q_1 q_2 = u_0 + u_1 2 + u_2 2^2 + \ldots + u_{x+y} 2^{x+y}$$

Die Koeffizienten c, v, w in den Ausdrücken p, q_1, q_2 können nur die Werthe 0 oder 1 haben, wogegen die Koeffizienten u in dem Ausdrucke $q_1 q_2$ beliebige Zahlwerthe annehmen können. Jede Potenz eines c, v oder w (jedoch nicht die eines u) ist also der ersten Potenz gleich und kann damit vertauscht werden. Die Koeffizienten u sind, wenn $y \geqq x$ ist (wenn also q_2 den grösseren der beiden Faktoren oder, eventuell, den dem anderen gleichen Faktor darstellt), entsprechend den schon in Nr. 10 aufgestellten Formeln,

$$\begin{array}{rcl}
u_0 &=& v_0 w_0 \\
u_1 &=& v_0 w_1 + v_1 w_0 \\
u_2 &=& v_0 w_2 + v_1 w_1 + v_2 w_0 \\
u_3 &=& v_0 w_3 + v_1 w_2 + v_2 w_1 + v_3 w_0 \\
\cdot & \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
u_x &=& v_0 w_x + v_1 w_{x-1} + \ldots + v_x w_0 \\
u_{x+1} &=& v_0 w_{x+1} + v_1 w_x + \ldots + v_x w_1 \\
u_{x+2} &=& v_0 w_{x+2} + v_1 w_{x+1} + \ldots + v_x w_2 \\
\cdot & \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
u_y &=& v_0 w_y + v_1 w_{y-1} + \ldots + v_x w_{y-x} \\
u_{y+1} &=& v_1 w_y + v_2 w_{y-1} + \ldots + v_x w_{y-x+1} \\
u_{y+2} &=& v_2 w_y + v_3 w_{y-1} + \ldots + v_x w_{y-x+2} \\
\cdot & \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
u_{x+y-2} &=& v_{x-2} w_y + v_{x-1} w_{y-1} + v_x w_{y-2} \\
u_{x+y-1} &=& v_{x-1} w_y + v_x w_{y-1} \\
u_{x+y} &=& v_x w_y
\end{array}$$

Da ohne Frage

$$q_1 > 2^x \quad \text{und} \quad < 2^{x+1}$$
$$q_2 > 2^y \quad \text{„} \quad < 2^{y+1}$$

also $$p = q_1 q_2 > 2^{x+y} \quad \text{„} \quad < 2^{x+y+2}$$

so ist $x + y < n + 1$ und $> n - 2$ oder $\leqq n$ und $\geqq n - 1$; die Summe $x + y$ der Exponenten der höchsten Potenzen in den Ausdrücken der beiden Faktoren q_1 und q_2 kann daher nur gleich n oder gleich $n - 1$ sein: es brauchen also nur solche Werthe von x und y in Betracht gezogen zu werden, welche dieser Bedingung entsprechen. Es kommen hiernach für ein gegebenes n nur $n - 1$ Werthe für x und y in Betracht, nämlich die folgenden. Für ein paares n

$$x = 1 \quad 1 \quad 2 \quad 2 \quad \ldots \quad \tfrac{1}{2}n - 1 \quad \tfrac{1}{2}n - 1 \quad \tfrac{1}{2}n$$
$$y = n - 1 \quad n - 2 \quad n - 2 \quad n - 3 \quad \ldots \quad \tfrac{1}{2}n + 1 \quad \tfrac{1}{2}n \quad \tfrac{1}{2}n$$

und für ein unpaares n

$$x = 1 \quad 1 \quad 2 \quad 2 \quad \ldots \quad \tfrac{1}{2}(n-1) \quad \tfrac{1}{2}(n-1)$$
$$y = n - 1 \quad n - 2 \quad n - 2 \quad n - 3 \quad \ldots \quad \tfrac{1}{2}(n+1) \quad \tfrac{1}{2}(n-1)$$

Da wir nur unpaare Zahlen p, q_1, q_2 in Betracht ziehen; so steht schon von vorn herein fest, dass die Koeffizienten c_0, v_0, w_0, u_0, sowie c_n, v_x und w_y gleich 1 sind, was sich übrigens auch aus der nachfolgenden Rechnung ergiebt. Transponiren wir in der Gleichung $q_1 q_2 = p$ das erste unpaare Glied $c_0 = 1$ auf die linke Seite; so bleibt links und rechts eine paare Grösse stehen; man hat

$$u_1 2 + u_2 2^2 + \ldots + u_{x+y} 2^{x+y} = c_1 2 + c_2 2^2 + \ldots + c_n 2^n$$

Jetzt und in allen späteren ähnlichen Fällen dividiren wir die Gleichung durch 2 und setzen das erste Glied der rechten Seite, wenn es ein solches ausser dem höchsten Gliede giebt, auf die linke Seite, sodass sich rechts immer ein paarer Ausdruck einstellt: man erhält also zunächst

$$u_1 - c_1 + u_2 2 + u_3 2^2 + \ldots + u_{x+y} 2^{x+y-1} = c_2 2 + c_3 2^2 + \ldots + c_n 2^{n-1}$$

Diese Gleichung erfordert, dass $u_1 - c_1 = v_0 w_1 + v_1 w_0 - c_1 = w_1 + v_1 - c_1$ paar sei. Die Grösse c_1 kann nur $= 0$ oder 1 sein: ist sie gleich 0; so muss entweder $v_1 = 0$, $w_1 = 0$, oder es muss $v_1 = 1$, $w_1 = 1$ sein. Ist $c_1 = 1$; so muss entweder $v_1 = 0$, $w_1 = 1$, oder es muss $v_1 = 1$, $w_1 = 0$ sein. Jedenfalls kommen für v_1, w_1 nur zwei Werthe in Betracht, mit welchen die Rechnung fortzuführen ist. Setzen wir den paaren Ausdruck $u_1 - c_1 = 2 r_1$, worin also r_1 einen bekannt gewordenen Werth hat; so folgt aus einer abermaligen Division der Gleichung durch 2 und Transposition von rechts nach links

$$r_1 + u_2 - c_2 + u_3 2 + u_4 2^2 + \ldots + u_{x+y} 2^{x+y-2} = c_3 2 + c_4 2^2 + \ldots + c_n 2^{n-2}$$

Jetzt muss wieder $r_1 + u_2 - c_2 = 2r_2$ sein und, da in $u_2 = v_0 w_2 + v_1 w_1 + v_2 w_0$ die Werthe von v_0, v_1, w_0, w_1 schon bekannt sind, auch r_1 und c_2 bekannt sind; so reduzirt sich diese Bedingung auf $w_2 + v_2 + d_2 = 2r_2$, worin d_2 eine bekannte Grösse ist. Ein paares d_2 verlangt entweder $v_2 = 0$, $w_2 = 0$, oder $v_2 = 1$, $w_2 = 1$. Ein unpaares d_2 verlangt $v_2 = 0$, $w_2 = 1$, oder $v_2 = 1$, $w_2 = 0$. Immer finden sich für v_2, w_2 nur zwei bestimmte Werthe. Nachdem hierdurch r_2 bekannt geworden, ergiebt eine abermalige Division mit 2

$$r_2 + u_3 - c_3 + u_4 2 + u_5 2^2 + \ldots + u_{x+y} 2^{x+y-3} = c_4 2 + c_5 2^2 + \ldots + c_n 2^{n-3}$$

Hierin ist wieder $r_2 + u_3 - c_3 = 2r_3$, woraus sich v_3, w_3 in zwei möglichen Ausdrücken ergiebt, und man erhält

$$r_3 + u_4 - c_4 + u_5 2 + u_6 2^2 + \ldots + u_{x+y} 2^{x+y-4} = c_5 2 + c_6 2^2 + \ldots + c_n 2^{n-4}$$

worin $r_3 + u_4 - c_4 = 2r_4$ zur Bestimmung von v_4, w_4 führt. Indem man in dieser Weise fortfährt und für v_5, w_5, für v_6, w_6 u. s. w. bis v_{x-1}, w_{x-1} Doppelausdrücke erhält, gelangt man zu der Gleichung

$$\begin{aligned} &r_{x-1} + u_x - c_x + u_{x+1} 2 + u_{x+2} 2^2 + \ldots + u_{x+y} 2^y \\ &= c_{x+1} 2 + c_{x+2} 2^2 + \ldots + c_n 2^{n-x} \end{aligned}$$

Die Bedingung $r_{x-1} + u_x - c_x = 2r_x$ liefert dann die Werthe von v_x, w_x in einem einfachen Ausdrucke, weil $v_x = 1$ sein muss.

Von dieser Stelle an setzt sich die Operation ganz in derselben Weise fort: allein in den nun folgenden Bedingungen

$$\begin{aligned} r_x + u_{x+1} - c_{x+1} &= 2r_{x+1} \\ r_{x+1} + u_{x+2} - c_{x+2} &= 2r_{x+2} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ r_{y-1} + u_y - c_y &= 2r_y \end{aligned}$$

erscheint immer nur eine einzige Unbekannte, nämlich erst w_{x+1}, dann w_{x+2} u. s. w., zuletzt w_y, man erhält also für diese Grössen lauter einfache bestimmte Werthe. Der Werth von w_y muss $= 1$ sein: fordert also die letzte Bedingung $w_y = 0$; so ist die Zerlegung der Zahl p nach den für v_0, v_1, $v_2 \ldots v_x$ und w_0, w_1, $w_2 \ldots w_y$ eingeführten speziellen Werthen unmöglich.

Ergiebt sich $w_y = 1$; so setzt sich das vorstehende Verfahren fort, es erscheinen aber in den späteren Gleichungen keine Unbekannten mehr, diese Gleichungen, nämlich

$$\begin{aligned} r_y + u_{y+1} - c_{y+1} + u_{y+2} 2 + u_{y+3} 2^2 + \ldots + u_{x+y} 2^{x-1} &= c_{y+2} 2 + \ldots + c_n 2^{n-y-1} \\ r_{y+1} + u_{y+2} - c_{y+2} + u_{y+3} 2 + u_{y+4} 2^2 + \ldots + u_{x+y} 2^{x-2} &= c_{y+3} 2 + \ldots + c_n 2^{n-y-2} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ r_{x+y-3} + u_{x+y-2} - c_{x+y-2} + u_{x+y-1} 2 + u_{x+y} 2^2 &= c_{x+y-1} 2 + \ldots + c_n 2^{n-x-y+2} \\ r_{x+y-2} + u_{x+y-1} - c_{x+y-1} + u_{x+y} 2 &= c_{x+y} 2 + \ldots + c_n 2^{n-x-y+1} \\ r_{x+y-1} + u_{x+y} - c_{x+y} &= c_{x+y+1} 2 + \ldots + c_n 2^{n-x-y} \end{aligned}$$

müssen sich durch die eingeführten speziellen Werthe der Unbekannten erfüllen. Bleibt eine derselben unerfüllt; so ist die Zerlegung nach jenen speziellen Fällen unmöglich: werden sie aber alle erfüllt; so stellen die

gefundenen Werthe eine Zerlegung der Zahl p dar. Da $x + y$ nur $= n$, oder $= n - 1$ sein kann; so werden die beiden letzten Gleichungen, da $c_n = 1$ ist, für $x + y = n$

$$\begin{aligned} r_{n-2} + u_{n-1} - c_{n-1} + u_n 2 &= c_n 2 = 2 \\ r_{n-1} + u_n - 1 &= 0 \end{aligned}$$

und für $x + y = n - 1$

$$\begin{aligned} r_{n-3} + u_{n-2} - c_{n-2} + u_{n-1} 2 &= c_{n-1} 2 + c_n 2^2 \\ r_{n-2} + u_{n-1} - c_{n-1} &= c_n 2 = 2 \end{aligned}$$

Die letzte Gleichung, welche in beiden Fällen die Grösse u_{x+y} enthält, dient, wenn $x = y$ ist, zur Bestimmung der beiden Koeffizienten v_x, w_y, kann aber, falls sie überhaupt möglich ist, nur ein einziges der beiden Werthpaare v_x, $w_y = 0$, 0 oder $= 1$, 1 und, wenn $y > x$ ist, nur einen bestimmten Werth für w_y liefern. Doppelwerthe finden sich mithin, wenn $x = y$ ist, für die Koeffizienten v_1, w_1, v_2, w_3 ... v_{x-1}, w_{x-1}, also an $x - 1$ Stellen, sodass, wenn alle diese Werthe mit den übrigen Werthen von v_0, w_0, w_x, w_{x+1} ... w_y mögliche Auflösungen lieferten, man 2^{x-1} mögliche Zerlegungen der Zahl p erhalten würde. Ist $y > x$; so könnten sich wegen der Doppelwerthigkeit von v_1, w_1 ... v_x, w_x überhaupt 2^x Zerlegungen ergeben.

Um die Rechnung an einem leichten Beispiele zu erläutern, sei $v = 21 = 1 + 0 . 2 + 1 . 2^2 + 0 . 2^3 + 1 . 2^4$, also $n = 4$. Die Grössen x und y können die Werthe $\begin{cases} x = 1\ 1\ 2 \\ y = 3\ 2\ 2 \end{cases}$ annehmen.

Für $x = 2$, $y = 2$ hat man, da $u_0 = 1$ ist,

$$u_1 2 + u_2 2^2 + u_3 2^3 + u_4 2^4 = 0 . 2 + 1 . 2^2 + 0 . 2^3 + 1 . 2^4$$
$$u_1 + u_2 2 + u_3 2^2 + u_4 2^3 = 1 . 2 + 0 . 2^2 + 1 . 2^3$$

$u_1 = w_1 + v_1 =$ paar, also entweder $v_1 = 0$, $w_1 = 0$, oder $v_1 = 1$, $w_1 = 1$.

Nimmt man zunächst $v_1 = 0$, $w_1 = 0$, also $u_1 = 1$; so kömmt

$$u_2 + u_3 2 + u_4 2^2 = 1 + 0 . 2 + 1 . 2^2$$

also $u_2 - 1 = w_2 + v_1 w_1 + v_2 - 1 = w_2 + v_2 - 1 =$ paar, mithin entweder $v_2 = 0$, $w_2 = 1$, oder $v_2 = 1$, $w_2 = 0$. Nimmt man $v_2 = 0$, $w_2 = 1$, also $u_2 - 1 = 0$; so ergiebt sich

$$u_3 + u_4 2 = 1 . 2$$

also $u_3 = w_3 + v_1 w_2 + v_2 w_1 + v_3 = w_3 + v_3 =$ paar, mithin entweder $v_3 = 0$, $w_3 = 0$, oder $v_3 = 1$, $w_3 = 1$. Nimmt man $v_3 = 0$, $w_3 = 0$, also $u_3 = 0$; so muss

$$u_4 = w_4 + v_1 w_3 + v_2 w_2 + v_3 w_1 + v_4 = w_4 + v_4 = 1$$

also entweder $v_4 = 0$, $w_4 = 1$, oder $v_4 = 1$, $w_4 = 0$ sein. Der letzte Fall $v_4 = 1$, $w_4 = 0$ ist jedoch ausgeschlossen, weil x nicht grösser als y werden, also der Faktor q_1 nicht mit einem höheren Gliede, als der Faktor q_2 schliessen darf. Die vorstehenden Werthe liefern die Zerlegung $q_1 = 1$, $q_2 = 1 + 0 . 2 + 1 . 2^2 + 0 . 2^3 + 1 . 2^4 = 21$.

Nimmt man statt der vorstehenden Werthe jetzt $v_1 = 1$, $w_1 = 1$, also $u_1 = 2$; so kömmt

$$1 + u_2 + u_3\,2 + u_4\,2^2 = 1 + 0\,.\,2 + 1\,.\,2^2$$

also $u_2 = w_2 + v_1 w_1 + v_2 = w_2 + 1 + v_2 =$ paar, mithin entweder $v_2 = 0$ $w_2 = 1$, oder $v_2 = 1$ $w_2 = 0$. Für $v_2 = 0$, $w_2 = 1$, also $u_2 = 2$ erhält man

$$1 + u_3 + u_4\,2 = 2$$

also $1 + u_3 = 1 + w_3 + 1 + v_3 = 2 + w_3 + v_3 =$ paar, mithin entweder $v_3 = 0$, $w_3 = 0$, oder $v_3 = 1$, $w_3 = 1$. Die Werthe $v_3 = 0$, $w_3 = 0$, also $u_3 = 1$ ergeben

$$1 + u_4 = 1$$

also $u_4 = w_4 + v_1 w_3 + v_2 w_2 + v_3 w_1 + v_1 = w_4 + v_1 = 0$, mithin $v_4 = 0$, $w_4 = 0$. Hieraus folgt die Zerlegung $q_1 = 1 + 1\,.\,2 = 3$ und $q_2 = 1 + 1\,.\,2 + 1\,.\,2^2 = 7$.

Wählte man für v_3 und w_3 die Werthe $v_3 = 1$, $w_3 = 1$, also $u_3 = 3$; so müsste

$$2 + u_4 = 1 \quad \text{oder} \quad 1 + u_4 = 0$$

sein. Da jetzt $u_4 = w_4 + 1 + 1 + v_4 = 2 + w_4 + v_4$ ist, also $1 + u_4 = 3 + w_4 + v_4 = 0$ eine Unmöglichkeit fordert; so können die Werthe $v_3 = 1$, $w_3 = 1$ mit den vorhergehenden Werthen von v_0, v_1, v_2, w_0, w_1, w_2 keine Zerlegung der Zahl 21 herbeiführen.

§. 14. Kennzeichnung der Theilbarkeit durch die Kongruenzen.

1) Wenn p eine beliebige Primzahl ist; so hat die Kongruenz $x^{p-1} \equiv 1 \bmod p$ bekanntlich primitive Wurzeln. Hiernach steht fest, dass, wenn jene Kongruenz keine primitive Wurzel hat, p keine Primzahl sein kann. Wir behaupten aber ferner, dass, wenn jene Kongruenz eine primitive Wurzel hat, d. h. wenn von irgend einer Zahl a die $(p-1)$-te Potenz die niedrigste ist, welche den Rest 1 ergiebt, p eine Primzahl sei. Denn ist a eine solche Zahl; so werden entweder die Reste der $p-1$ Potenzen a^1, a^2, a^3 . . . a^{p-1} sämmtlich verschieden sein, mithin alle Zahlen 1, 2, 3 . . . $(p-1)$ enthalten, oder es werden sich von einem gewissen Reste r_1 an die folgenden Reste periodisch wiederholen, sodass r_1, r_2, r_3 . . . r_α resp. $= r_{\alpha+1}$, $r_{\alpha+2}$, $r_{\alpha+3}$ . . . $r_{2\alpha}$ etc. sind. Der zweite Fall kann nicht eintreten, weil sich bei fortgesetzter Bildung der Potenzen von a über die $(p-1)$-te hinaus alle Reste von a^1, a^2, a^3 . . . wiederholen, mithin der Rest 1 von a^{p-1} oder von a^0 in einer der späteren Perioden, mithin auch in der ersten Periode r_1, r_2 . . . r_α stehen, also der Rest einer Potenz a^x sein wird, deren Exponent $x < p-1$ ist, was der Voraussetzung widerspricht. Angenommen nun, der erste Fall trete ein, unter den $p-1$ Resten der ersten $p-1$ Potenzen von a erscheinen also alle Zahlen 1, 2, 3 . . . $(p-1)$. Wäre p eine zusammengesetzte und b eine Zahl $< p$, welche mit p ein gemeinschaftliches Maass hat;

so müsste die Wurzel a nothwendig ebenfalls ein gemeinschaftliches Maass mit p haben, weil sonst unmöglich $a^x \equiv b$ sein könnte. Hat aber a ein gemeinschaftliches Maass mit p und ist c eine zu p relativ prime Zahl $< p$; so kann unmöglich $a^x \equiv c$ sein. Hiernach können, wenn p eine zusammengesetzte Zahl ist, unter den Resten von a, mag nun a mit p ein gemeinschaftliches Maass haben, oder nicht, nicht alle Zahlen $1, 2, 3 \ldots (p-1)$ vorkommen: findet Letzteres also nach der Voraussetzung statt; so muss p eine Primzahl sein.

Wäre der Rest von x^{p-1} für irgend einen Werth von $x = a$ nicht $= 1$; so würde auch p keine Primzahl sein können, da für jede Primzahl p jene Potenz für jeden Werth von x den Rest 1 haben muss. Wenn m die Anzahl der zu p relativ primen Zahlen $< p$ (einschliesslich der 1) bezeichnet; so ist bekanntlich für jede zu p relativ prime Wurzel a $a^m \equiv 1 \ mod\ p$, gleichviel, ob p eine Primzahl ist oder nicht. Für eine Primzahl ist $m = p - 1$, für eine zusammengesetzte Zahl aber ist $m < p - 1$; für einen zusammengesetzten Model p kann also die Kongruenz $x^{p-1} \equiv 1$ niemals primitive Wurzeln haben, d. h. es wird unbedingt der Rest einer niedrigeren Potenz schon $= 1$ sein, und ausserdem kann möglicherweise der Rest von a^{p-1} verschieden von 1 sein.

Aus dem Vorstehenden ergiebt sich, dass die Existenz oder Nichtexistenz einer primitiven Wurzel der Kongruenz $x^{p-1} \equiv 1 \ mod\ p$ ein ausschliessliches Merkmal für die Unzerlegbarkeit oder die Zusammengesetztheit des Models p ist.

2) Dass die Zahl 2 keine primitive Wurzel einer Primzahl von der Form $p = 2^n + 1$, wenn $n > 4$, also $p > 17$ ist, sein kann, leuchtet ein, da $2^n \equiv -1 \ mod\ p$, mithin schon $2^{n+1} \equiv 1 \ mod\ p$ ist, folglich alle Potenzen $2^{n+1}, 2^{n+2}, 2^{n+3}, \ldots$ bis $2^{p-1} = 2^{2^n}$ den Rest 1 haben, sodass 2^{p-1} nicht die niedrigste Potenz ist, welche den Rest 1 darbietet. Die Zahl 2 kömmt also als primitive Wurzel nicht in Betracht.

Kennt man eine Zahl a, von welcher sich nachweisen lässt, dass sie unbedingt eine primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \ mod\ p$ für die Primzahl p als Model sein muss; so entscheiden die Reste der Potenzen $a^1, a^2, a^3 \ldots a^{p-1}$ darüber, ob p eine Primzahl ist, oder nicht: p ist dann und nur dann eine Primzahl, wenn unter diesen Resten der Werth 1 in letzter Stelle und zwar lediglich an dieser Stelle vorkömmt.

Die Bildung der Reste dieser $p - 1$ Potenzen würde für grosse Werthe von p, z. B. für $p = 2^{32} + 1$ unausführbar sein: hat jedoch p die Form $2^n + 1$, worin $n = 2^\alpha$ ist; so bedarf es nicht der Kenntniss aller jener Reste, sondern nur sehr weniger derselben. Denn ist die r-te die niedrigste Potenz von a, deren Rest $= 1$ ist; so muss r ein Faktor von $p - 1 = 2^n$, also ebenfalls eine Potenz von 2 sein, man muss also $r = 2^m$ haben. Hiernach kommen nur diejenigen Potenzen von a, deren Exponenten r die Werthe $2^0, 2^1, 2^2, 2^3 \ldots 2^n$ haben, in Betracht. Jede folgende dieser Potenzen wie $a^{2^{m+1}}$ ist aber das Quadrat der vorhergehenden a^{2^m}. Demzufolge braucht man nur $n - 1 = 2^\alpha - 1$ Quadraturen auszuführen. Jede Quadratur aber ist, weil man nur den Rest der zu quadrirenden Zahl zu quadriren braucht, eine Multiplikation von Zahlen,

welche kleiner als p sind. So brauchte man z. B. zur Entscheidung, ob $2^{32} + 1$ eine Primzahl ist, nur 31 Quadraturen vorzunehmen. Kömmt unter den gedachten $n - 1$ Resten der Rest 1 an letzter Stelle und lediglich an dieser Stelle vor; so ist p eine Primzahl, sonst aber nicht.

Bildet man nicht die kleinsten positiven, sondern die kleinsten absoluten Reste, welche $\leqq \frac{p-1}{2}$ sind; so wird, wenn p eine Primzahl ist, in der vorletzten Stelle der eben genannten Reste der Rest -1 erscheinen, und, wenn p eine zusammengesetzte Zahl ist, kann in einer früheren Stelle der Rest -1 erscheinen. Jedenfalls ist p keine Primzahl, wenn in einer früheren als der vorletzten Stelle der Rest -1 erscheint. Immer bedarf es jetzt einer Quadratur weniger, als vorhin, und die zu quadrirenden Zahlen sind im Allgemeinen nur halb so gross, als die früheren.

Nach §. 11 Nr. 2, c ist 3 eine primitive Wurzel jeder Primzahl von der für p vorausgesetzten Form (ausgenommen den Fall $p = 2^1 + 1 = 3$). Wenn sich also durch die eben erwähnten 31, resp. 30 Reste 3 nicht als eine primitive Wurzel ausweis't, ist p keine Primzahl.

Die Anzahl der Quadraturen 3^2, $(3^2)^2 = 3^4$, $(3^4)^2 = 3^8$ etc. lässt sich unter die Anzahl 2^n noch weiter herabmindern, wenn man das schon früher von uns gebrauchte Verfahren der Restbildung in Anwendung bringt, also die kleinsten absoluten Reste nach der Tafel

$$\begin{array}{cccccc} 1 & 2 & 4 & 8 & \ldots & 2^{n-1} \\ 3 & 2.3 & 4.3 & 8.3 & \ldots & 2^{n-1}.3 \\ 3^2 & 2.3^2 & 4.3^2 & 8.3^2 & \ldots & 2^{n-1}.3^2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}$$

zusammengestellt denkt. In dieser Tafel, welche die Reste aller Potenzen von 3 bis zur Potenz vom Grade $\frac{p-1}{2} = 2^{n-1}$ umfasst, enthält jede Horizontalreihe n Glieder und die ganze Tafel 2^{n-1} Zahlen, also $\frac{2^{n-1}}{n} = \frac{p-1}{2n}$ Horizontalreihen. Die erste Reihe umfasst ausser der Zahl $2^0 = 1$ die $n - 1$ ersten Potenzen von 2. Da dieselben sämmtlich $\leqq \frac{1}{2}(p-1)$ sind; so stellen sie immer kleinste absolute Reste nach dem Model $p = 2^n + 1$ dar, wie gross auch dieser Model oder der Exponent n sein möge. Ausserdem ist diese, wie jede andere Horizontalreihe eine zyklische Reihe absoluter Reste, da die nächst höhere Potenz $2^n \equiv -1$ ist, also wieder den absoluten Rest 1 hat. Sobald sich also an irgend einer Stelle der Tafel der Rest 1 einstellt, müssen sich in derselben Reihe die Reste 2, 4, 8 ... in den nächstfolgenden Stellen und sodann zyklisch über die erste Stelle hinweg wiederholen, d. h. es muss die ganze erste Reihe in derselben Reihenfolge, wenn auch mit einem anderen Anfangsgliede wiederkehren, und demzufolge muss das erste Glied der fraglichen

Reihe, welches der Rest einer Potenz von 3 ist, eine Potenz von 2 sein, oder man muss $3^x \equiv 2^y$ haben, worin $x \leq \frac{p-1}{2n} - 1$ und $y \leq n - 1$ ist.

Wenn sich eine Horizontalreihe wiederholt, muss sich offenbar auch die nächstfolgende und jede spätere Reihe wiederholen, weil die je folgende aus der vorhergehenden durch Multiplikation mit 3 entsteht. Der Exponent x des Anfangsgliedes der Reihe, in welcher sich die erste Reihe wiederholt, muss also ein Faktor von $\frac{p-1}{2n}$ sein. Da $p-1$ und n Potenzen von 2 sind; so ist auch $\frac{p-1}{2n}$ eine Potenz von 2; es kömmt also nur darauf an, die Reste der Potenzen 3, 3^2, 3^4, 3^8 ... von 3, welche sich durch fortgesetzte Quadratur ergeben, bis hinauf zur Potenz vom Grade $\frac{p-1}{2n}$ zu bilden und nachzusehen, ob sich darunter eine Potenz von 2 befinde. Diess erfordert, da $\frac{p-1}{2n} = 2^{n-\alpha-1}$ ist, nur $n - \alpha - 1$ Quadraturen, also α Operationen weniger, als vorher. Für $p = 2^{32} + 1$ würde man hiernach nur $32 - 5 - 1 = 26$ Quadraturen auszuführen brauchen. Kömmt unter diesen $n - \alpha - 1$ Resten eine Potenz von 2 an letzter Stelle und lediglich an dieser Stelle vor; so ist p eine Primzahl, entgegengesetztenfalls aber nicht.

Die 32 Potenzen von 2, welche die kleinsten absoluten Reste der ersten Horizontalreihe bilden, sind

$2^0 =$	1,	$2^1 =$	2,	$2^2 =$	4,
$2^3 =$	8,	$2^4 =$	16,	$2^5 =$	32,
$2^6 =$	64,	$2^7 =$	128,	$2^8 =$	256,
$2^9 =$	512,	$2^{10} =$	1 024,	$2^{11} =$	2 048,
$2^{12} =$	4 096,	$2^{13} =$	8 192,	$2^{14} =$	16 384,
$2^{15} =$	32 768,	$2^{16} =$	65 536,	$2^{17} =$	131 072,
$2^{18} =$	262 144,	$2^{19} =$	524 288,	$2^{20} =$	1 048 576,
$2^{21} =$	2 097 152,	$2^{22} =$	4 194 304,	$2^{23} =$	8 388 608,
$2^{24} =$	16 777 216,	$2^{25} =$	33 554 432,	$2^{26} =$	67 108 864,
$2^{27} =$	134 217 728,	$2^{28} =$	268 435 456,	$2^{29} =$	536 870 912,
$2^{30} =$	1 073 741 824,	$2^{31} =$	2 147 483 648,		

indem die nächstfolgende Potenz $2^{32} = 4\,294\,967\,296 \equiv -1$ ist oder wieder den ersten kleinsten absoluten Rest 1 hat (während, wie schon erwähnt, 2^{33} und jede höhere Potenz von 2 den positiven Rest 1 darbietet). Für die in Betracht kommenden Potenzen von 3 ergeben sich durch Quadratur folgende kleinsten Reste, worunter wir die negativen durch das Minuszeichen kenntlich gemacht haben.

$$3^{2^1} \equiv 9,\quad 3^{2^2} \equiv 81,\quad 3^{2^3} \equiv 6\,561,$$
$$3^{2^4} \equiv 43\,046\,721,\quad 3^{2^5} \equiv -1\,765\,839,\quad 3^{2^6} \equiv 41\,116\,299,$$
$$3^{2^7} \equiv -624\,249\,363,\quad 3^{2^8} \equiv 971\,279\,080,\quad 3^{2^9} \equiv -75\,014\,051,$$
$$3^{2^{10}} \equiv 608\,691\,190,\quad 3^{2^{11}} \equiv 1\,749\,935\,127,\quad 3^{2^{12}} \equiv -2\,037\,409\,525,$$
$$3^{2^{13}} \equiv -1\,607\,683\,125,\quad 3^{2^{14}} \equiv -399\,572\,477,\quad 3^{2^{15}} \equiv 719\,770\,568,$$
$$3^{2^{16}} \equiv -748\,503\,391,\quad 3^{2^{17}} \equiv -546\,245\,097,\quad 3^{2^{18}} \equiv 1\,317\,807\,019,$$
$$3^{2^{19}} \equiv 602\,309\,062,\quad 3^{2^{20}} \equiv -1\,870\,115\,302,\quad 3^{2^{21}} \equiv 585\,815\,656,$$
$$3^{2^{22}} \equiv 1\,156\,501\,984,\quad 3^{2^{23}} \equiv -704\,657\,994,\quad 3^{2^{24}} \equiv 1\,315\,015\,236,$$
$$3^{2^{25}} \equiv 1\,781\,920\,693,\quad 3^{2^{26}} \equiv -543\,668\,582.$$

Da der letzte dieser Reste der Potenzen von 3 keine Potenz von 2 ist; so kann $2^{32}+1$ keine Primzahl sein. Hiermit ist die Zusammengesetztheit der letzteren Zahl auf einem kurzen und direkten, alles Probiren ausschliessenden Wege dargethan.

Um übrigens dieses Verfahren an einer Primzahl zu konstatiren; so hat man für $p = 2^8+1 = 257$ folgende Reste der Potenzen von 3 bis zum Grade $2^{8-3-1} = 2^4$

$$3^{2^1} \equiv 9,\quad 3^{2^2} \equiv 81,\quad 3^{2^3} \equiv -121,\quad 3^{2^4} \equiv -8.$$

Da der letzte und nur der letzte dieser vier Reste eine Potenz von 2 darstellt; so entscheiden diese wenigen Operationen über die Thatsache, dass 257 eine Primzahl ist. Wir bemerken noch, dass die nächsten Quadraturen bis zum Grade 2^8 die Reste $3^{2^5} \equiv 64$, $3^{2^6} \equiv -16$, $3^{2^7} \equiv -1$, $3^{2^8} \equiv 1$ ergeben, sodass die Potenz vom Grade 2^7 die niedrigste ist, welche den Rest -1 ergiebt, und die Potenz vom Grade 2^8 die niedrigste, welche den Rest $= 1$ hervorbringt.

3) Das vorstehende Verfahren zur Ermittlung, ob eine gegebene Zahl p eine Primzahl sei, oder nicht, lässt sich für die mittelst Kegelschnitte konstruirbaren Kreistheilungen verallgemeinern. Für diese muss p nach §. 12 Nr. 7 die Form $2^\alpha 3^\beta + 1$ haben. Kann man nun auf irgend einem Wege eine Zahl a ermitteln, welche, wenn p eine Primzahl ist, nothwendig eine primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \bmod p$ sein muss; so kömmt es nur darauf an zu konstatiren, dass thatsächlich $a^{p-1} \equiv 1$ ist, und dass keine der niedrigeren Potenzen von a, deren Grad ein Faktor von $p-1 = 2^\alpha 3^\beta$ ist, den Rest 1 aufweis't. Alle diese Potenzen von a sind aber entweder Quadraturen von a, oder von a^3, oder von $a^{3^2} = a^9$ oder von $a^{3^3} = a^{27}$, oder schliesslich von a^{3^β}. Man hat also nur eine mässige Menge von Quadraturen zu bilden, um zu entscheiden, ob p eine Primzahl sei, oder nicht.

Beispielsweise hat $p = 2^5 . 3 + 1 = 97$ zugleich die Form $5 . 19 + 2$. Demnach ist nach §. 11 Nr. 4, c die Zahl 5 ein quadratischer Nichtrest

für 97, und dieselbe wird nach §. 11 Nr. 7 eine primitive Wurzel nach 97 als Primzahl sein, insofern nicht $5^{2^{5-1}} = 5^{2^4} \equiv -1$ ist. In der That ist $5^{16} \equiv 36$, also nicht $\equiv -1$, und demzufolge ist 5 eine primitive Wurzel nach 97, wenn 97 eine Primzahl ist. Die Frage, ob 97 eine Primzahl sei, wird hiernach entschieden, wenn sich herausstellt, dass von den Potenzen, welche durch Quadrirung aus 5 und aus $5^3 = 125$ hervorgehen, die Potenz $5^{2^5 \cdot 3}$ die einzige ist, die den Rest 1 liefert. Man findet $5^2 \equiv 25$, $5^{2^2} \equiv 43$, $5^{2^3} \equiv 6$, $5^{2^4} \equiv 36$, $5^{2^5} \equiv 35$ und $5^3 \equiv 28$, $5^{2 \cdot 3} \equiv 8$, $5^{2^2 \cdot 3} \equiv 64$, $5^{2^3 \cdot 3} \equiv 22$, $5^{2^4 \cdot 3} \equiv -1$, $5^{2^5 \cdot 3} \equiv 1$, und demzufolge ist 97 eine Primzahl.

4) Schliesslich bemerke ich, dass ich die Vermuthung hege, dass, gleichwie die um eine Einheit vermehrten ersten Dignitäten, nämlich $2^0 + 1 = 2$, $2^1 + 1 = 3$, $2^2 + 1 = 5$, $2^{2^2} + 1 = 2^4 + 1 = 17$, $2^{2^{2^2}} + 1 = 2^{16} + 1 = 65\,537$ Primzahlen sind, auch alle folgenden ähnlichen Dignitäten, zunächst also $2^{2^{16}} + 1 = 2^{65536} + 1$ Primzahlen liefern, dass mir jedoch der Beweis nicht gelungen ist. Sollte sich diese Vermuthung bestätigen; so würde damit eine allgemeine Formel für eine besondere Klasse von Primzahlen gegeben sein.

§. 15. Die Reste der Potenzen eines Binoms.

Wenn ${}^nB_m$ den m-ten Binomialkoeffizienten der n-ten Potenz darstellt; so ergiebt sich leicht für beliebige positive ganze Werthe von r, n, x die allgemeine Beziehung

$$(25)\quad (a+b)\{a^r - {}^nB_1 a^{r-1} b + {}^{n+1}B_2 a^{r-2} b^2 - {}^{n+2}B_3 a^{r-3} b^3 + \ldots (-1)^x {}^{n+x-1}B_x a^{r-x} b^x\}$$
$$= \{a^{r+1} - {}^{n-1}B_1 a^r b + {}^nB_2 a^{r-1} b^2 - {}^{n+1}B_3 a^{r-2} b^3 + \ldots (-1)^{x+1} {}^{n+x-1}B_{x+1} a^{r-x} b^{x+1}\} + (-1)^x {}^{n+x}B_{x+1} a^{r-x} b^{x+1}$$

oder auch

$$(26)\quad (a-b)\{a^r + {}^nB_1 a^{r-1} b + {}^{n+1}B_2 a^{r-2} b^2 + \ldots + {}^{n+x-1}B_x a^{r-x} b^x\}$$
$$= \{a^{r+1} + {}^{n-1}B_1 a^r b + {}^nB_2 a^{r-1} b^2 + \ldots + {}^{n+x-1}B_{x+1} a^{r-x} b^{x+1}\} - {}^{n+x}B_{x+1} a^{r-x} b^{x+1}$$

Auf der rechten Seite ist das erste Glied ebenso gebildet wie der zweite Faktor auf der linken Seite: bezeichnet man den letzteren mit $F(r, n, x) = F$; so ist das gedachte Glied $F(r+1, n-1, x+1) = F_1$, und man hat, indem man im zweiten Gliede auf der rechten Seite ${}^{n+x}B_{x+1} = {}^{n+x}B_{n-1}$ setzt,

$$(a+b)\, F = F_1 + (-1)^x {}^{n+x}B_{n-1} a^{r-x} b^{x+1}$$

also auch

$$F = \frac{1}{a+b}\{F_1 + (-1)^x {}^{n+x}B_{n-1} a^{r-x} b^{x+1}\}$$

Setzt man hierin für F_1 seinen Werth

$$F_1 = \frac{1}{a+b}\{F_2 + (-1)^{x+1}\ {}^{n+x}B_{n-2}\ a^{r-x}\ b^{x+2}\}$$

worin $F_2 = F(r+2, n-2, x+2)$ ist; so erhält man

$$F = \frac{1}{(a+b)^2}\{F_2 + (-1)^{x+1}\ {}^{n+x}B_{n-2}\ a^{r-x}\ b^{x+2} + (-1)^x\ {}^{n+x}B_{n-1}\ (a+b)\ a^{r-x}\ b^{x+1}\}$$

Beim Übergange von einer Funktion F zu der nächsten erniedrigen sich die Potenzen der darin erscheinenden Binomialkoeffizienten, bis man endlich in der Funktion F_{n-1} auf die Binomialkoeffizienten ${}^1B_1, {}^2B_2, {}^3B_3$ u. s. w., welche sämmtlich $= 1$ sind, und in der Funktion F_n auf die Binomialkoeffizienten ${}^0B_1, {}^1B_2, {}^2B_3$ u. s. w., welche sämmtlich $= 0$ sind, stösst, sodass man $F_n = a^{r+n}$ erhält. Hierdurch wird

$$(27)\quad F = a^r - {}^nB_1\ a^{r-1}b + {}^{n+1}B_2\ a^{r-2}b^2 - \ldots (-1)^x\ {}^{n+x-1}B_x\ a^{r-x}\ b^x$$
$$= \frac{1}{(a+b)^n}\{a^{r+n} + (-1)^{x+n-1}\ {}^{n+x}B_0\ a^{r-x}\ b^{n+x} + (-1)^{n+x-2}\ {}^{n+x}B_1\ (a+b)\ a^{r-x}\ b^{n+x-1} + (-1)^{n+x-3}\ {}^{n+x}B_2\ (a+b)^2\ a^{r-x}\ b^{n+x-2} + \ldots + (-1)^{x+1}\ {}^{n+x}B_{n-2}\ (a+b)^{n-2}\ a^{r-x}\ b^{x+2} + (-1)^x\ {}^{n+x}B_{n-1}\ (a+b)^{n-1}\ a^{r-x}\ b^{x+1}\}$$

Besonders beachtenswerth an der algebraischen Beziehung zwischen zwei mit Binomialkoeffizienten behafteten Reihen ist die Thatsache, dass die auf der rechten Seite stehende Reihe durch $(a+b)^n$ theilbar ist, dass also der Quotient, wenn a und b ganze Zahlen sind, ebenfalls eine ganze Zahl ist.

Für den speziellen Fall $x = r$ ergiebt sich, indem man $r = p - n$ setzt und unter p eine unpaare Zahl versteht,

$$(28)\quad a^{p-n} - {}^nB_1\ a^{p-n-1}b + {}^{n+1}B_2\ a^{p-n-2}b^2 - \ldots (-1)^{n-1}\ {}^{p-1}B_{p-n}\ b^{p-n}$$
$$= \frac{1}{(a+b)^n}\{a^p + b^p - {}^pB_1\ (a+b)\ b^{p-1} + {}^pB_2\ (a+b)^2\ b^{p-2} - \ldots (-1)^{n-1}\ {}^pB_{n-1}\ (a+b)^{n-1}\ b^{p-n+1}\}$$

Einige in dieser Formel liegenden speziellen Fälle sind für $n = 1, 2, 3$

$$(29)\quad a^{p-1} - a^{p-2}b + a^{p-3}b^2 - a^{p-4}b^3 + \ldots - ab^{p-2} + b^{p-1} = \frac{a^p + b^p}{a+b}$$

$$(30)\quad a^{p-2} - 2a^{p-3}b + 3a^{p-4}b^2 - 4a^{p-5}b^3 + \ldots + (p-2)ab^{p-3} - (p-1)b^{p-2} = \frac{a^p + b^p - p(a+b)b^{p-1}}{(a+b)^2}$$

$$(31)\quad a^{p-3} - 3a^{p-4}b + 6a^{p-5}b^2 + 10a^{p-6}b^3 + \ldots + \frac{(p-1)(p-2)}{1\cdot 2}b^{p-3} = \frac{1}{(a+b)^3}\left\{a^p + b^p - p(a+b)b^{p-1} + \frac{p(p-1)}{1\cdot 2}(a+b)^2 b^{p-2}\right\}$$

Untersuchen wir jetzt den Rest der Potenz des Binoms $a + b$ vom Grade $p - n$ nach der unpaaren Primzahl p als Model; so ist in der Formel

$$(a+b)^{p-n} = a^{p-n} + {}^{p-n}B_1\, a^{p-n-1}\, b + {}^{p-n}B_2\, a^{p-n-2}\, b^2 + \ldots + b^{p-n}$$

irgend ein Binomialkoeffizient

$$\begin{aligned} {}^{p-n}B_m &= \frac{(p-n)\,(p-n-1)\,\ldots\,(p-n-m+1)}{1\,.\,2\,\ldots\,m} \\ &= \frac{A\,p + (-1)^m\,(n+m-1)\,(n+m-2)\,\ldots\,(n+1)\,n}{1\,.\,2\,\ldots\,m} \\ &= \frac{A\,p}{1\,.\,2\,\ldots\,m} + (-1)^m\ {}^{n+m-1}B_m \end{aligned}$$

Da im ersten Gliede auf der rechten Seite kein Faktor des Nenners in der Primzahl p enthalten ist; so muss der ganze Nenner in A aufgehen, man hat also

$$(32) \qquad {}^{p-n}B_m \equiv (-1)^m\ {}^{n+m-1}B_m \ mod\ p$$

und daher

$$(33) \qquad (a+b)^{p-n} \equiv a^{p-n} - {}^{n}B_1\, a^{p-n-1}\, b + {}^{n+1}B_2\, a^{p-n-2}\, b^2 - \ldots (-1)^{n-1}\ {}^{p-1}B_{p-n}\, b^{p-n}$$

Die rechte Seite dieser Kongruenz ist der linken Seite der Gl. (28) vollkommen gleich, man hat also für den Model p

$$(34) \qquad (a+b)^{p-n} \equiv \frac{1}{(a+b)^n}\,\{a^p + b^p - {}^{p}B_1\,(a+b)\,b^{p-1} + {}^{p}B_2\,(a+b)^2\,b^{p-2} - \ldots (-1)^{n-1}\ {}^{p}B_{n-1}\,(a+b)^{n-1}\,b^{p-n+1}\}$$

Für $n = 1, 2, 3$ ist daher, wenn man zugleich beachtet, dass nach dem Fermatschen Lehrsatze $(a+b)^{p-1} \equiv 1$ ist

$$(a+b)^{p-1} \equiv \frac{a^p + b^p}{a+b} \equiv 1$$

$$(a+b)^{p-2} \equiv \frac{a^p + b^p - p\,(a+b)\,b^{p-1}}{(a+b)^2}$$

$$(a+b)^{p-3} \equiv \frac{1}{(a+b)^3}\left\{a^p + b^p - p\,(a+b)\,b^{p-1} + \frac{p\,(p-1)}{1\,.\,2}\,(a+b)^2 b^{p-2}\right\}$$

Die rechten Seiten dieser Kongruenzen ergeben sich rekursorisch aus einander durch die Relationen

$$\frac{a^p + b^p}{a+b} = C_1$$

$$\frac{a^p + b^p - p\,(a+b)\,b^{p-1}}{(a+b)^2} = \frac{1}{a+b}\,(C_1 - p\,b^{p-1}) = C_2$$

$$\frac{1}{(a+b)^3}\left\{a^p + b^p - p\,(a+b)\,b^{p-1} + \frac{p\,(p-1)}{1\,.\,2}\,(a+b)^2\,b^{p-2}\right\} = \frac{1}{a+b}\left(C_2 + \frac{p\,(p-1)}{1\,.\,2}\,b^{p-2}\right) = C_3$$

u. s. w., man hat also

$$(a+b)^{p-1} \equiv C_1 \equiv 1$$

$$(a+b)^{p-2} \equiv \frac{1}{a+b}(C_1 - p\,b^{p-1}) = C_2$$

$$(a+b)^{p-3} \equiv \frac{1}{a+b}\left(C_2 + \frac{p(p-1)}{1.2}\,b^{p-2}\right) = C_3$$

$$(a+b)^{p-4} \equiv \frac{1}{a+b}\left(C_3 - \frac{p(p-1)(p-2)}{1.2.3}\,b^{p-3}\right) = C_4$$

u. s. w. Für $b = 1$ werden alle Potenzen von b gleich 1, und man hat generell

$$(35)\quad (a+1)^{p-n} \equiv \frac{1}{a+1}\left\{C_{n-1} + (-1)^{n-1}\frac{p(p-1)\ldots(p-n+2)}{1.2\ldots(n-1)}\right\}$$

So erhält man z. B. für $p = 7$, $a = 2$, $b = 1$

$$C_1 = \frac{1}{3}(2^7 + 1) = 43,$$

$$C_2 = \frac{1}{3}(43 - 7) = 12,$$

$$C_3 = \frac{1}{3}\left(12 + \frac{7.6}{1.2}\right) = 11,$$

$$C_4 = \frac{1}{3}\left(11 - \frac{7.6.5}{1.2.3}\right) = -8,$$

$$C_5 = \frac{1}{3}\left(-8 + \frac{7.6.5.4}{1.2.3.4}\right) = 9,$$

$$C_6 = \frac{1}{3}\left(9 - \frac{7.6.5.4.3}{1.2.3.4.5}\right) = -4$$

und in der That, ist $3^6 = 43 \equiv 1$, $3^5 = 12 \equiv 5$, $3^4 = 11 \equiv 4$, $3^3 \equiv -8 \equiv 6$, $3^2 \equiv 9 \equiv 2$, $3^1 \equiv -4 \equiv 3$ *mod* 7.

Wenn man in der Formel (34) $n = p - m$ setzt, schliesslich aber wieder n statt m schreibt, nimmt sie die Gestalt

$$(36)\quad (a+b)^n \equiv \frac{1}{(a+b)^{p-n}}\{a^p + b^p - {}^pB_1(a+b)b^{p-1} + {}^pB_2(a+b)^2b^{p-2} - \ldots (-1)^n\,{}^pB_{p-n-1}\,(a+b)^{p-n-1}\,b^{n+1}\}$$

an. Substituirt man in den Formeln (25), (27) bis (36) für b eine negative Grösse; so verschwindet der Zeichenwechsel in den Reihen: statt (36) erhält man

$$(37)\quad (a-b)^n \equiv \frac{1}{(a-b)^{p-n}}\{a^p - b^p - {}^pB_1(a-b)b^{p-1} - {}^pB_2(a-b)^2b^{p-2} - \ldots - {}^pB_{p-n-1}\,(a-b)^{p-n-1}\,b^{n+1}\}$$

Dass man in allen diesen Formeln a und b vertauschen kann, ist selbstredend.

Entwickelt man die Potenz a^p nach dem binomischen Lehrsatze in der Form

$$\begin{aligned} a^p &= [b + (a - b)]^p \\ &= b^p + {}^pB_1\,(a-b)\,b^{p-1} + {}^pB_2\,(a-b)^2\,b^{p-2} + \ldots \\ &\quad + {}^pB_{p-n-1}\,(a-b)^{p-n-1}\,b^{n+1} + {}^pB_{p-n}\,(a-b)^{p-n}\,b^n + \ldots \\ &\quad + {}^pB_{p-1}\,(a-b)^{p-1}\,b + (a-b)^p \end{aligned}$$

und zerschneidet die Reihe auf der rechten Seite an einer beliebigen Stelle hinter dem $(p-n)$-ten Gliede, bezeichnet darauf den ersten Theil, welcher $p-n$ Glieder umfasst, mit A und den zweiten Theil, welcher $n+1$ Glieder umfasst, mit B, sodass also $a^p = A + B$ ist; so findet man leicht statt der Formel (37)

$$(38) \qquad (a-b)^n \equiv \frac{B}{(a-b)^{p-n}}$$

$$(39)\ \text{auch} \qquad b^{p-n-1} \equiv \frac{A}{b^{n+1}}$$

Entwickelt man a^p nach der Formel

$$\begin{aligned} a^p &= [-b + (a+b)]^p \\ &= -b^p + {}^pB_1\,(a+b)\,b^{p-1} - {}^pB_2\,(a+b)^2\,b^{p-2} + \ldots \\ &\quad (-1)^{n+1}\,{}^pB_{p-n-1}\,(a+b)^{p-n-1}\,b^{n+1} + (-1)^n\,{}^pB_{p-n}\,(a+b)^{p-n}\,b^n + \ldots \\ &\quad - {}^pB_1\,(a+b)^{p-1}\,b + (a+b)^p \end{aligned}$$

und setzt den Inbegriff der ersten $p-n$ Glieder gleich A', sowie den Inbegriff der letzten $n+1$ Glieder gleich B', sodass wiederum $a^p = A' + B'$ ist; so ergiebt sich

$$(40) \qquad (a+b)^n \equiv \frac{B'}{(a+b)^{p-n}}$$

$$(41) \qquad b^{p-n-1} \equiv -\frac{A'}{b^{n+1}}$$

§. 16. Die Anzahl und Höhe der Primzahlen.

1) Der Wilsonsche Lehrsatz sagt, dass, wenn p eine Primzahl ist, die Grösse $1 \cdot 2 \cdot 3 \ldots (p-1) + 1$ durch p theilbar ist, und dass, wenn p eine zusammengesetzte Zahl ist, die gedachte Grösse nicht durch p theilbar ist. Man kann statt des zweiten Theiles dieses Satzes auch die Behauptung aussprechen, dass, wenn p eine zusammengesetzte Zahl mit Ausnahme der Zahl 4 ist, das Produkt $1 \cdot 2 \ldots (p-1) = q$ durch p theilbar ist. Denn wenn $p_1, p_2, \ldots p_r$ alle unterhalb p liegenden Primzahlen sind; so kann, wenn p eine zusammengesetzte Zahl ausser 4 ist, q nur ein Produkt von der Form $p_1^{m_1}\,p_2^{m_2}\,p_3^{m_3} \ldots p_r^{m_r}$ sein und p kann ebenfalls nur die Form $p_1^{n_1}\,p_2^{n_2}\,p_3^{n_3} \ldots p_3^{n_r}$ haben, worin jedes $m_x \geqq n_x$ ist. Alsdann ist aber

$$\frac{q}{p} = p_1^{m_1-n_1}\,p_2^{m_2-n_2}\,p_3^{m_3-n_3} \ldots p_r^{m_r-n_r}$$

eine ganze Zahl, also q durch p theilbar.

2) Über die mögliche Grösse einer Primzahl p ertheilt der Wilsonsche Lehrsatz keine Auskunft, auch nicht darüber, ob über jede Grenze hinaus Primzahlen existiren. Folgende Betrachtung giebt hierüber Aufschluss. Angenommen, es gebe r unpaare Primzahlen, welche der Reihe nach durch $p_1, p_2, \ldots p_r$ dargestellt sind, indem alle dazwischen liegenden Zahlen zusammengesetzte Zahlen sind; so wird jede Zahl von der Form $q = p_1, p_2, \ldots p_r + 2^s$, worin der Exponent s einen beliebigen ganzen Werth hat, durch keine der Primzahlen $p_1, p_2, \ldots p_r$ theilbar sein, sie wird also entweder selbst eine Primzahl sein, oder aus lauter Primfaktoren bestehen, welche unter den Primzahlen $p_1, p_2, \ldots p_r$ nicht vorkommen, welche also $> p_r$ und $< p_1 p_2 \ldots p_r + 2^s$ sind. Hieraus folgt, indem man $n = 0$ nimmt, dass es nothwendig Primzahlen giebt, welche zwischen den Grenzen p_r und $p_1 p_2 \ldots p_r + 1$ liegen, dass es also, da dieser Schluss, wenn man immer die dem letzten Falle entsprechende grösste Primzahl für p_r nimmt, ohne Ende fortgesetzt werden kann, unendlich viel Primzahlen von unbeschränkter Höhe giebt.

Die letztere Betrachtung hat auch in der Hinsicht ein Interesse, dass sie zwei relativ prime Zahlen bezeichnet: denn es liegt auf der Hand, dass, wenn $p_1, p_2, \ldots p_r$ ganz beliebige unpaare Primzahlen > 1 sind, die beiden Zahlen

$$p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r} \quad \text{und} \quad p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r} + 2^s$$

worin die Exponenten $m_1, m_2, \ldots m_r$ und $n_1, n_2, \ldots n_r$, sowie s sämmtlich > 0 sind, keinen gemeinschaftlichen Faktor haben. So sind z. B. 3 und $3 + 2^s = 5, 7, 11, 19, 35, 67$ u. s. w., auch $3 . 5 = 15$ und $15 + 2^s = 17, 19, 23, 31, 47, 79, 143$ u. s. w. je zwei relativ prime Zahlen.

Für einen Werth von s, für welchen nicht gerade $p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r} - p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r} = 2^s$ ist, sind auch die beiden Zahlen

$$p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r} \quad \text{und} \quad p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r} - 2^s$$

relativ prim.

Wenn $p_1, p_2, \ldots p_r$ nicht r beliebige, sondern die r ersten Primzahlen bezeichnen; so muss auch der absolute Werth von $p_1, p_2 \ldots p_r - 2^s$ entweder eine Primzahl (möglicherweise jedoch auch $= 1$) sein, oder eine Primzahl enthalten, welche $> p_r$ ist. So ist z. B. für $3 . 5 - 2^s$ für $s = 3$ $15 - 8 = 7 > 5$ und für $s = 4$ $3 . 5 - 2^4 = -1$.

3) Ist für die letztere Bedeutung der Grössen $p_1, p_2, \ldots p_r$ das Produkt $p_1 p_2 \ldots p_r = p$; so ist p relativ prim zu $p + 2$ und auch zu $p + 4$, es ist aber auch $p + 2$ relativ prim zu $p + 4 = (p + 2) + 2$. Demnach haben die drei Zahlen p, $p + 2$, $p + 4$ lauter verschiedene Primfaktoren $> p_r$. Hieraus folgt, dass sowohl $p + 2$, als auch $p + 4$ entweder eine Primzahl ist, oder lauter Primfaktoren enthält, welche $> p_r$ sind und in $p + 2$ und $p + 4$ verschiedene Werthe haben, dass also in den beiden Zahlen $p + 2$ und $p + 4$ jedenfalls zwei verschiedene Primzahlen $> p_r$ enthalten sind.

Das Nämliche gilt von den beiden Zahlen $p + 2$ und $p - 2$. So ist z. B. für $p_1, p_2, p_3 = 3, 5, 7$ $p = 3 . 5 . 7 = 105$, $105 + 2 = 107$ und $105 - 2 = 103$ eine Primzahl.

4) Wenn p das Produkt beliebiger Potenzen der aufeinander folgenden unpaaren Primzahlen $p_1, p_2, \ldots p_r$, also $p = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ ist; so haben zwei Zahlen von der Form $q_1 = p + 2a_1$ und $q_2 = p + 2a_2$, da nun $q_2 = q_1 + 2(a_2 - a_1)$ ist, alle diejenigen Faktoren miteinander gemein, welche gemeinschaftliche Faktoren von q_1 und $a_2 - a_1$ sind und sonst keine. Wenn $a_2 \leqq p_r$ ist; so kann die Grösse $a_2 - a_1$ nur Primfaktoren aus der Reihe der $p_1, p_2, \ldots p_r$ enthalten, also nur solche können gemeinschaftliche Faktoren von q_1 und q_2 sein. Nach Abscheidung dieser gemeinschaftlichen Faktoren muss q_2 noch Primfaktoren enthalten, welche $> p_r$ sind und welche nur in dem speziellen Falle, wo der abgeschiedene Faktor die Potenz einer Primzahl ist, $= p_r$ sein können (wie z. B. in $q_1 = 3 . 5 = 15$ und $q_2 = q_1 + 2 . 5 = 25 = 5^2$ der gemeinschaftliche Faktor von q_1 und q_2 den Werth $p_r = 5$ hat).

Wenn die Faktoren von p die ersten Potenzen der Primzahlen $p_1, p_2, \ldots p_r$ sind, also $q_1 = p + 2a_1$, $q_2 = p + 2a_2 = q_1 + 2(a_2 - a_1)$ ist; so sei b der gemeinschaftliche Faktor von q_1 und q_2, also der gemeinschaftliche Faktor von q_1 und $a_2 - a_1$, welcher nur ein Produkt von Primzahlen $p_1, p_2, \ldots p_r$ (oder deren Potenzen) sein kann. Nach Abscheidung dieses Faktors b aus dem Werthe von q_2 ist der andere Faktor von q_2 entweder eine Primzahl $p_s > p_r$ und $< \frac{q_2}{b}$, d. h. $< \frac{p + 2a_2}{b}$, oder er ist das Produkt von mehreren Primzahlen, also mindestens von 2 Primzahlen $p_s = p_r + 2c$, $p_t = p_r + 2d$, welche $> p_r$ sind, von denen also die grössere $p_t = \frac{q_2}{p_s} = \frac{q_2}{p_r + 2c} < \frac{q_2}{p_r}$ oder $< \frac{p + 2a_2}{p_r}$ oder $< p_1 p_2 \ldots p_{r-1} + \frac{2a_2}{p_r}$ oder $\leqq p_1 p_2 \ldots p_{r-1}$ ist.

Bildet man daher alle unpaaren Zahlen $p + 2$, $p + 4$, $p + 6$, $\ldots$ $p + 2p_r$; so sind einige davon Primzahlen, von den übrigen enthalten keine zwei einen gemeinschaftlichen Primfaktor, welcher $> p_r$ wäre; jeder darin vorkommende Primfaktor, welcher $> p_r$ ist, kömmt also nur einer einzigen dieser Zahlen zu. Es enthält aber jede dieser Zahlen, wenn sie nicht schon selbst eine Primzahl ist, einen solchen Primfaktor: denn die beiden Zahlen p und $p + 2a_2$ haben die in a_2 enthaltenen unpaaren Primfaktoren aus der Reihe der $p_1, p_2, \ldots p_r$ auf erster Potenz gemein. Sind p_{x_1}, p_{x_2} u. s. w. diese Primfaktoren und ihr Produkt $b = p_{x_1} p_{x_2} \ldots$, also $p = b . \frac{p}{b}$ und $p + 2a_2 = b . \frac{p}{b} + 2^x bc = b\left(\frac{p}{b} + 2^x c\right)$; so enthält von dem Faktor $\frac{p}{b} + 2^x c$ das erste Glied keinen der Primfaktoren $p_{x_1}, p_{x_2}, \ldots$ und das zweite Glied kann in c wohl von den Primfaktoren $p_{x_1}, p_{x_2}, \ldots$ etliche, jedoch keinen der übrigen Primfaktoren aus der Reihe $p_1, p_2, \ldots p_r$, also keinen Faktor des ersten

Gliedes $\frac{p}{b}$ enthalten, weil b das gemeinschaftliche Maass von p und a_2 erschöpft. Hiernach muss also der Faktor $\frac{p+2a_2}{b} = \frac{p}{b} + 2^x c$ der Zahl $p + 2a_2$ entweder selbst eine Primzahl sein, welche dann $< \frac{p+2p_r}{b}$ oder $< \frac{(p_1 p_2 \ldots p_{r-1} + 2)p_r}{b}$ ist, oder jener Faktor muss aus lauter Primfaktoren bestehen, welche, wenn sie nicht zufällig alle einander gleich und gleich p_r sind, sämmtlich $> p_r$ und $< \frac{p+2a_2}{b(p_r+2c)}$ mithin $< \frac{p+2a_2}{bp_r}$ oder $< \frac{p}{bp_r} + \frac{2a_2}{bp_r}$ und, da a_2 höchstens den Werth p_r und b mindestens den Werth 1 annimmt, $\leqq p_1 p_2 \ldots p_{r-1} + 2$ sind.

Hieraus geht hervor, dass jede der p_r Zahlen $p + 2$, $p + 4$, $\ldots$ $p + 2p_r$ mindestens eine Primzahl liefert, welche zwischen p_r und $p + 2p_r$ liegt, dass es also in diesem Zwischenraume der Zahlenreihe, welcher sich von p_r bis $(p_1 p_2 \ldots p_{r-1} + 2)p_r$ erstreckt, mindestens p_r oder unter Berücksichtigung des Falles, wo $p + 2p_r = p_r^x$, also $p_1 p_2 \ldots p_{r-1} + 2 = p_r^{x-1}$ ist, mindestens $p_r - 1$ Primzahlen giebt.

Beispielsweise hat man für die ersten 4 Primzahlen 3, 5, 7, 11 $p = 3.5.7.11 = 1155$, $p + 2 = 1157 = 13.89$, $p + 4 = 1159 = 19.61$, $p + 6 = 1161 = 3^3.43$, $p + 8 = 1163$, $p + 10 = 1165 = 5.233$, $p + 12 = 1167 = 3.389$, $p + 14 = 1169 = 7.167$, $p + 16 = 1171$, $p + 18 = 1173 = 3.17.23$, $p + 20 = 1175 = 5^2.47$, $p + 22 = 1177 = 11.107$. Jede dieser 11 Zahlen liefert mindestens eine Primzahl, welche > 11 und $\leqq 1177$ ist. Diejenigen Zahlen, welche ein gemeinschaftliches Maass b mit p haben, liefern Primfaktoren, welche $< \frac{1177}{b}$ sind.

Nach Vorstehendem bedingt die Existenz der r Primzahlen $p_1, p_2, \ldots p_r$ die fernere Existenz von $p_r - 1$ Primzahlen $> p_r$, also die Existenz von überhaupt $r + p_r - 1 = r_1$ Primzahlen. Werden die ersten r_1 Primzahlen mit $p_1, p_2, \ldots p_{r_1}$ bezeichnet; so bedingen dieselben die fernere Existenz von $p_{r_1} - 1$, im Ganzen also die Existenz von $r_1 + p_{r_1} - 1 = r_2$ Primzahlen $p_1, p_2, \ldots p_{r_2}$. Hieraus folgt, dass die wachsende Anzahl der Primzahlen eine immer grössere Anzahl höherer Primzahlen bedingt. So bedingt die eine Primzahl 3 noch $3 - 1 = 2$ Primzahlen > 3 ($3 + 2 = 5$ liefert 5, $3 + 4 = 7$ liefert 7, $3 + 6 = 9 = 3^2$ liefert keine Primzahl > 3), überhaupt also $1 + 2 = 3$ Primzahlen. Die ersten 3 Primzahlen 3, 5, 7 bedingen noch $7 - 1 = 6$, im Ganzen $3 + 6 = 9$ Primzahlen. Die ersten 9 Primzahlen 3, 5, 7, 11, 13, 17, 19, 23, 29 bedingen noch $29 - 1 = 28$, im Ganzen $9 + 28 = 37$ Primzahlen. Die ersten 37 Primzahlen 3, 5, $\ldots$ 167 bedingen noch $167 - 1 = 166$, im Ganzen $37 + 166 = 203$ Primzahlen u. s. f.

5) Zwischen den beiden unpaaren Zahlen p und q liegen $q - p - 1$ ganze und $\frac{q-p}{2} - 1$ unpaare Zahlen. Setzt man $p = p_1 p_2 \ldots p_r$ und $q = p_1 p = p_1^2 p_2 \ldots p_r$; so liegen zwischen p und q überhaupt $\frac{q-p}{2} - 1 = \frac{p(p_1-1)}{2} - 1$ unpaare Zahlen. Wenn $p_1, p_2, \ldots p_r$ die Reihe der unpaaren Primzahlen darstellt, also $p_1 = 3$ ist; so liegen zwischen p und q $p - 1$ unpaare Zahlen, welche $> p$ und $< q$ sind. Die unter diesen Zahlen vorkommenden theilbaren Zahlen können nur die Primfaktoren $p_1, p_2, \ldots p_r$ haben, oder sie müssen neben solchen Faktoren Primfaktoren enthalten, welche $> p_r$ und $< \frac{p}{2}$ sind. Ermittelt man also alle aus den Faktoren $p_1, p_2, \ldots p_r$ zusammengesetzten Zahlen, welche $> p$ und $< q$ sind, und findet man ihre Anzahl $= m$; so müssen zwischen p und q nothwendig $p - 1 - m$ Primzahlen und solche Zahlen liegen, welche einen Primfaktor $> p_r$ enthalten. Zur Ermittlung der Grösse m kann man entweder die Kombinationen von $p_1, p_2, \ldots$ bilden, oder folgendermaassen verfahren. Man setzt $p_1 = 3$, $p_2 = 5 = 3^{\alpha_2}$, $p_3 = 7 = 3^{\alpha_3}$, $p_4 = 11 = 3^{\alpha_4}, \ldots$ $p_r = 3^{\alpha_r}$, also $p = 3^{1+\alpha_2+\alpha_3+\ldots+\alpha_r}$ und $q = 3^{2+\alpha_2+\alpha_3+\ldots+\alpha_r}$. Irgend eine aus den Faktoren $p_1, p_2 \ldots p_r$ zusammengesetzte Zahl $p_1^{x_1} p_2^{x_2} \ldots p_r^{x_r}$ ist dann $= 3^{x_1+\alpha_2 x_2+\alpha_3 x_3+\ldots+\alpha_r x_r}$, und die Aufgabe fordert die Erfüllung der beiden Ungleichheiten

$$x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \ldots + \alpha_r x_r \begin{matrix} > 1 + \alpha_2 + \alpha_3 + \ldots + \alpha_r \\ < 2 + \alpha_2 + \alpha_3 + \ldots + \alpha_r \end{matrix}$$

oder, wenn man $x_n = \frac{\log p_n}{\log 3}$ setzt,

$$x_n \log p_1 + x_2 \log p_2 + x_3 \log p_3 + \ldots + x_r \log p_r \begin{matrix} > \log p \\ < \log p + \log p_1 \end{matrix}$$

Die Anzahl der Auflösungen dieser Ungleichheiten durch ganze Zahlen $x_1, x_2, \ldots x_r$ ist der Werth von m. So hat man z. B. für $p = 3 \cdot 5 = 15$ und $q = 3^2 \cdot 5 = 45$ zwischen 15 und 45 überhaupt $15 - 1 = 14$ unpaare Zahlen. Hiervon sind nur 2, nämlich $3 \cdot 3 \cdot 3 = 27$ und $5 \cdot 5 = 25$ aus den Faktoren 3 und 5 zusammengesetzt und > 15 und < 45, mithin $14 - 2 = 12$ Zahlen theils Primzahlen, theils mit Faktoren > 5 behaftet. In der That, hat man zwischen 15 und 45 die 8 Primzahlen 17, 19, 23, 29, 31, 37, 41, 43 und die 4 Zahlen $21 = 3 \cdot 7$, $33 = 3 \cdot 11$, $35 = 5 \cdot 7$, $39 = 3 \cdot 13$ mit den Primfaktoren 7, 11, 13, welche > 5 sind. Mit Hülfe der Logarithmen erhält man die Ungleichheiten

$$x_1 \log 3 + x_2 \log 5 > \log 15 < \log 45$$

oder in gemeinen Logarithmen

$$0{,}477\, x_1 + 0{,}699\, x_2 > 1{,}176 < 1{,}653$$

Dieselben lassen nur 2 Auflösungen

$$x_1 = 3 \quad 0$$
$$x_2 = 0 \quad 2$$

zu (indem $x_1 = 2$, $x_2 = 1$, was dem Falle $3^2 . 5 = 45$ entspricht, die linke Seite $= 1{,}653$, also dem Maximum 1,653 genau gleich macht, während sie kleiner als dieses Maximum bleiben muss).

Die grösste Primzahl, welche in eine zwischen p und $q = p_1 p$ liegende theilbare Zahl eintreten kann, ist $< \frac{q}{p_1}$ also $< p$. Kennt man also alle Primzahlen, welche $< p$ sind, und wird die grösste derselben mit $p_s = 3^{a_s}$ bezeichnet; so ergeben sich alle zwischen p und q liegenden theilbaren Zahlen durch die Bedingung, dass $p_1^{x_1} p_2^{x_2} \ldots p_s^{x_s} > p$ und $< q$ sein muss, oder auch durch die Auflösung der Ungleichheiten

$$x_1 \log p_1 + x_2 \log p_2 + \ldots + x_s \log p_s > \log p < \log q$$

Ist n die Anzahl dieser Auflösungen; so ist $p - 1 - n$ die Anzahl der zwischen p und q liegenden Primzahlen, und man erhält alle diese Primzahlen, indem man von den zwischen p und q liegenden unpaaren Zahlen die den genannten n Auflösungen entsprechenden theilbaren Zahlen ausschliesst. Diese Primzahlen bilden die natürliche Verlängerug der Primzahlenreihe über die Zahl p_s hinaus.

In dem Beispiele $p = 3 . 5 = 15$, $q = 3^2 . 5 = 45$ sind die unter p liegenden Primzahlen 3, 5, 7, 11, 13, also $p_s = p_5 = 13$. Die Ungleichheiten

$$0{,}477\, x_1 + 0{,}699\, x_2 + 0{,}845\, x_3 + 1{,}041\, x_4 + 1{,}114\, x_5 > 1{,}176 < 1{,}653$$

werden durch die 6 Auflösungen

$$\begin{array}{llllll} x_1 = 3 & 0 & 1 & 1 & 1 & 0 \\ x_2 = 0 & 2 & 0 & 0 & 0 & 1 \\ x_3 = 0 & 0 & 1 & 0 & 0 & 1 \\ x_4 = 0 & 0 & 0 & 1 & 0 & 0 \\ x_5 = 0 & 0 & 0 & 0 & 1 & 0 \end{array}$$

erfüllt, zwischen 15 und 45 liegen also $15 - 1 - 6 = 8$ Primzahlen.

Die letzteren Auflösungen erleichtern sich durch Feststellung der höchsten Werthe $y_1, y_2, \ldots y_s$, welche die ganzen Zahlen $x_1, x_2, \ldots x_s$ annehmen können. Für den höchsten Werth y_n irgend eines x_n muss $p_n^{y_n} < q$ sein, man hat also für y_n die grösste unter $\frac{\log q}{\log p_n}$ liegende ganze Zahl zu nehmen und demzufolge kommen für $x_1, x_2, \ldots$ nur folgende Werthe in Betracht.

$$x_1 = 0, 1, 2, 3 \ldots y_1 < \frac{\log q}{\log p_1}$$
$$x_2 = 0, 1, 2, 3 \ldots y_2 < \frac{\log q}{\log p_2}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x_s = 0, 1, 2, 3 \ldots y_s < \frac{\log q}{\log p_s}$$

Selbstredend kann man für q jedes Produkt von der Form $p_1^{\alpha_1} p_2^{\alpha_2} p_r^{\alpha_r}$ annehmen und danach die aufzulösenden Ungleichheiten leicht feststellen, um die zwischen p und q liegenden Primzahlen, deren Anzahl $\frac{q-p}{2} - 1 - n$ ist, zu bestimmen.

Für die praktische Ermittlung des Werthes von n wird sich die Bildung der Kombinationen aus den Faktoren $p_1, p_2, \ldots$ als das einfachere Verfahren empfehlen, wenn man dabei folgendermaassen systematisch zu Werke geht. Für irgend eine Kombination A sei a die nächste unpaare Zahl, welche $> \frac{p}{A}$ ist, und b sei die nächste unpaare Zahl, welche $< \frac{q}{A}$ ist. Alsdann kommen von denjenigen Kombinationen, deren Anfangsglieder gleich A sind, die folgenden

$$A\,a \quad A(a+2) \quad A(a+4) \quad \ldots \quad Ab$$

in Betracht, deren Anzahl

$$\frac{b-a}{2} + 1 = t$$

ist. Von diesen sind diejenigen auszuschliessen, deren letzter Faktor eine der von a bis b vorkommenden theilbaren Zahlen ist. Diese Zahlen sind sämmtlich bekannt, da jede derselben nach der Voraussetzung $< \frac{q}{A}$ oder $< \frac{p_1 p}{A}$ ist, aber p_1 die niedrigste Primzahl, also $\leqq A$, mithin die fragliche Zahl $< p$ ist. Ist nun t' die Anzahl der bekannten theilbaren Zahlen von a bis b (einschliesslich dieser beiden Grenzwerthe); so enthält die vorstehende Reihe $t - t'$ theilbare Zahlen, deren letzter Faktor grösser ist, als der höchste Primfaktor von A, sie stellt also alle zulässigen Kombinationen mit dem Anfangsprodukte A dar. (Ergäbe sich $a \geqq \frac{q}{A}$; so wäre A eine unzulässige, zu kleine Kombination; ergäbe sich $a \leqq \frac{p}{A}$; so wäre A eine unzulässige, zu grosse Kombination.) Ausser der sehr leichten Ermittlung des Werthes von a und b bedarf es also keiner Rechnung. In Erwägung, dass in allen Kombinationen der Primfaktoren $p_1, p_2 \ldots$, also sowohl in A, als auch in Aa auf den letzten Faktor immer nur ein gleicher oder ein grösserer, niemals ein kleinerer folgen darf (um alle Wiederholungen derselben theilbaren Zahlen zu vermeiden), lassen sich nun die verschiedenen Werthe von A ohne alle Rechnung niederschreiben, und die Bestimmung der zugehörigen Werthe von a und b ist eine geringfügige Arbeit. Nimmt man beispiesweise $p = 3 \cdot 5 \cdot 7 = 105$, $q = 3p = 315$, werden also die Primzahlen, welche unterhalb 105 liegen, als bekannt vorausgesetzt; so ergeben sich die zwischen 105 und 315 liegenden theilbaren und Primzahlen aus folgender leicht verständlichen Zusammenstellung

		t	t'
$3.3.3.3 \times 3$		1	0
$3.3.3 \times 5 \ldots$	11	4	1
$3.3.5 \times 5$		1	0
$3.3 \times 13 \ldots$	33	11	5
$3.5 \times 9 \ldots$	19	6	2
$3.7 \times 7 \ldots$	13	4	1
$5.5 \times 5 \ldots$	11	4	1
5.7×7		1	0
$3 \times 37 \ldots$	103	34	18
$5 \times 23 \ldots$	61	20	10
$7 \times 17 \ldots$	43	14	6
$11 \times 11 \ldots$	27	9	4
$13 \times 13 \ldots$	23	6	2
17×17		1	0
		116	50

Hiernach ist $n = 116 - 50 = 66$ und $p - 1 - n = 105 - 1 - 66 = 38$, es giebt also unter den zwischen 105 und 315 liegenden 104 Zahlen 66 theilbare und 38 Primzahlen. Die 66 theilbaren Zahlen gehen aus der vorstehenden Zusammenstellung hervor, indem sich z. B. für $A = 3.5$ die $t = 6$ Kombinationen $3.5.9$, $3.5.11$, $3.5.13$, $3.5.15$, $3.5.17$, $3.5.19$ ergeben, wovon die $t' = 2$ Kombinationen $3.5.9$ und $3.5.15$ auszuschliessen sind, sodass die $t - t' = 4$ theilbaren Zahlen $3.5.11$, $3.5.13$, $3.5.17$, $3.5.19$ zurückbleiben. Nach Ausscheidung aller dieser 66 theilbaren Zahlen sind die zurückbleibenden die 38 Primzahlen, welche zwischen 105 und 315 liegen.

6) Aus Vorstehendem ergiebt sich folgendes Verfahren zur Ermittlung aller Primzahlen in ununterbrochener Reihenfolge. Wenn eine Reihe aufeinander folgender Primzahlen bekannt ist; so bezeichnen wir dieselben durch $p_1, p_2, \ldots p_s$ und ermitteln durch Multiplikation der ersten Zahlen $p_1, p_2 \ldots$ dieser Reihe das niedrigste Produkt $p_1 p_2 \ldots p_r$, welches grösser ist, als die grösste Primzahl p_s der gegebenen Reihe. Ist nun $p_s < p_1 p_2 \ldots p_r$; so nehmen wir die höchste Primzahl dieses Produktes für die vorher mit p_r bezeichnete Zahl und setzen $p = p_1 p_2 \ldots p_r$ und $q = p_1 p$. Das vorstehende Verfahren lehrt dann die Anzahl und die Werthe aller zwischen p und q liegenden Primzahlen als unmittelbare Verlängerung der Primzahlenreihe jenseit des Werthes p_s kennen.

Der Fall, dass es zwischen p und $q = 3p$ keine Primzahlen gäbe, sodass also p_s die höchste Primzahl nicht nur unter p, sondern auch unter $3p$ wäre, wird wohl niemals eintreten: träte er aber ein; so würde man $q = p_1^2 p$ nehmen und danach die zu erfüllenden Ungleichheiten leicht bestimmen können. Lägen auch zwischen p und $p_1^2 p$ keine Primzahlen; so würde man $q = p_1^3 p$ nehmen. Endlich wird ein Werth von der

Form $q = p_1^n p$ die Fortsetzung der Reihe der Primzahlen liefern, da die Zahl derselben nach Obigem unbegrenzt ist.

Übrigens kann man für q jedes der in voriger Nummer bezeichneten Produkte nehmen.

7) Obgleich das Verfahren in Nr. 5 den kleinsten Aufwand von Ziffern erfordert; so ist doch das nachstehende Verfahren zur Ermittlung der zwischen gegebenen unpaaren Grenzen a und b liegenden Primzahlen leichter auszuführen. Es kommen die aufeinander folgenden unpaaren Zahlen $r = 3, 5, 7, 9, 11$ u. s. w. bis zu der Zahl, welche zunächst $\leqq \sqrt{b}$ ist, in Betracht. Ist für irgend eine der Zahlen r die Zahl u_r die zunächst über $\frac{a}{r}$ liegende oder ihr gleiche unpaare Zahl, also $u_r \geqq \frac{a}{r}$ und das Produkt $r u_r = a + \beta_r$, also die Differenz $\beta_r = r u_r - a$; so beachte man, dass die Reihe der Zahlen

$$\begin{array}{llll} r u_r, & r(u_r + 2), & r(u_r + 4), & r(u_r + 6) \text{ u. s. w.} \\ = a + \beta_r, & a + \beta_r + 2r, & a + \beta_r + 4r, & a + \beta_r + 6r \text{ u. s. w.} \end{array}$$

ist. Für das letzte Glied einer solchen Reihe ist $r(u_r + 2n) \leqq b$, also $n \leqq \frac{1}{2}\left(\frac{b}{r} - u_r\right)$ oder auch $\leqq \frac{b - a - \beta_r}{2r}$. Übrigens darf im ersten Gliede der Faktor u_r nicht $< r$ werden: sobald also in den späteren Reihen Diess eintritt, also sobald $r \leqq \sqrt{a}$ wird, ist fortwährend $u_r = r$ und daher $\beta_r = r^2 - a$ zu nehmen. Der höchste Werth von r ist $\leqq \sqrt{b}$. Hiernach bilden wir für $r = 3, 5, 7, 9$ etc. durch einfache Addition bezw. der Differenz 6, 10, 14, 18 etc. die Zahlenreihen

$$\begin{array}{llll} \beta_3 & \beta_3 + 6 & \beta_3 + 12 & \beta_3 + 18 \ldots \\ \beta_5 & \beta_5 + 10 & \beta_5 + 20 & \beta_5 + 30 \ldots \\ \beta_7 & \beta_7 + 14 & \beta_7 + 28 & \beta_7 + 42 \ldots \end{array}$$

u. s. w. und vergegenwärtigen uns, dass alle über a liegenden theilbaren unpaaren Zahlen den Werth von a um die in diesen Reihen stehenden Zahlen überschreiten und dass jede Reihe eine steigende arithmetische Progression bildet, dass mithin die kleinsten über a liegenden theilbaren Zahlen aus den ersten Gliedern dieser Reihen erkannt werden können. Enthalten nun diese Reihen alle paaren Zahlen 2, 4, 6, 8 u. s. w.; so giebt es keine über a liegenden Primzahlen; jede fehlende paare Zahl $2n$ bezeichnet aber eine Primzahl $a + 2n$.

Wenn die unterhalb $\sqrt{b}$ liegenden Primzahlen bekannt sind, brauchen für r nur diese Primzahlen gesetzt zu werden, da die unpaaren Werthe von r, welche theilbar sind, doch nur Wiederholungen der in den übrigen Reihen enthaltenen Werthe ergeben können. Sind die unter $\sqrt{a}$ liegenden, nicht aber die zwischen $\sqrt{a}$ und $\sqrt{b}$ liegenden Primzahlen bekannt; so hat man für r die ersteren Primzahlen und sodann die höheren unpaaren

Zahlen zu setzen. Um z. B. die über $a = 1001$ bis zu einer unbestimmten Obergrenze b liegenden Primzahlen zu ermitteln, hat man wegen $\sqrt{a} = 31{,}6\ldots$ für r, wenn die Primzahlen bis 31 bekannt sind, erst die 10 Werthe von $r = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ und sodann die unpaaren Zahlen 33, 35, 37 etc. zu setzen. Für die bestimmte Obergrenze 2001 würden wegen $\sqrt{2001} = 44{,}7$ nur noch die unpaaren Zahlen bis 43 oder, wenn die Primzahlen bis 43 bekannt sind, nur noch die drei Primzahlen 37, 41, 43 in Betracht kommen. Die Werthe α_3 bis α_{31} sind 335, 201, 143 ... 33, also die Werthe der Grössen β_3 bis β_{31} nach der Formel $r\alpha_r - a$ und der Grössen β_{37} bis β_{43} nach der Formel $r^2 - a$ die ersten Glieder der nachstehenden Reihen, welche wir bei dem Werthe 64 abgebrochen haben.

r												
3	4	10	16	22	28	34	40	46	52	58	64	. . .
5	4	14	24	34	44	59	64	.	.	.		
7	0	14	28	42	56	70	.	.	.			
11	2	24	46	68	.	.	.					
13	0	26	52	78	.	.	.					
17	2	36	70	.	.	.						
19	6	44	82	.	.	.						
23	34	80	.	.	.							
29	14	102	.	.	.							
31	22	84	.	.	.							
37	368	442	.	.	.							
41	680	762	.	.	.							
43	848	934	.	.	.							

Aus diesen Reihen folgt, dass wegen $\beta_7 = 0$ 1001 selbst eine theilbare Zahl ist und die fehlenden Zahlen 8, 12, 18, 20, 30, 32, 38, 48, 50, 54, 60 u. s. w. die zunächst über 1001 liegenden Primzahlen 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061 u. s. w. in ununterbrochener Reihenfolge ergeben.

Wenn weder eine untere, noch eine obere Grenze gegeben ist, nimmt jede Reihe der theilbaren Zahlen die Form r^2, $r^2 + 2r$, $r^2 + 4r$ u. s. w. an. Die erste Reihe für $r = 3$, nämlich 9, 15, 21 u. s. w. sagt dann, dass alle zwischen 3 und 9 liegenden unpaaren Zahlen 5, 7 Primzahlen sind. Mit dieser Erkenntniss ergeben die drei Reihen

9	15	21	27	33	39	45	51
25	35	45	55				
49	63	77					

dass zwischen 9 und 49 die Primzahlen 11, 13, 17, 23, 29, 31, 37, 41, 43, 47 liegen. Aldann lehren die Reihen

9	15	21	. . .
25	35	45	. . .
49	63	77	. . .
121	142	164	. . .
169	195	221	. . .
. .	. .	. .	. . .
961	993	1055	. . .

die Primzahlen erkennen, welche zwischen 49 und 961 liegen u. s. f.

8) Wenn $p_1, p_2, \ldots p_r$ der Anfang der Reihe der aufeinander folgenden Primzahlen und $p = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ ist; so ist $q = p \mp 2^n$ nach Nr. 1 entweder eine Primzahl, oder besteht aus lauter Primfaktoren, welche $> p_r$ sind. Bezeichnet x die grösstmögliche Menge von Primfaktoren von q; so muss, weil p_r kleiner als jeder derselben ist, $p_r^x < q$, also $x \log p_r < \log q$, mithin $x < \frac{\log q}{\log p_r}$ sein. Hiernach ist x die kleinste ganze Zahl, welche unter $\frac{\log q}{\log p_r}$ liegt. Hat daher dieser Bruch einen Werth $\leqq 2$; so ist $x = 1$, die Zahl q kann also dann nur einen einzigen Faktor haben, d. h. sie ist selbst eine Primzahl $> p_r$. Diese Bedingung verlangt, dass $\log q$ oder $\log (p \mp 2^n) \leqq 2 \log p_r \leqq \log p_r^2$ oder dass $p \mp 2^n \leqq p_r^2$ sei.

Gilt in der Formel für q das positive Zeichen, wird also $q = p + 2^n$ genommen; so ist q eine Primzahl, wenn $2^n \leqq p_r^2 - p$ ist. Die Erfüllung dieser Bedingung setzt voraus, dass $p_r > p_1 p_2 \ldots p_{r-1}$ sei, weil sonst die Grösse auf der rechten Seite nicht positiv bleiben kann. Diese Voraussetzung findet nur für die Reihe $p = 3 . 5$ statt, indem schon für die Reihe $3 . 5 . 7$ die höchste Primzahl $7 < 3 . 5$ ist. Für die erstere Reihe $p = 3 . 5$ ist $p_r^2 - p = 5^2 - 3 . 5 = 10$. Jede unter 10 liegende Potenz von 2, also 2, 4, 8, kann daher für 2^n genommen werden, und liefert in der Formel $p + 2^n$ eine Primzahl > 7, nämlich $3 . 5 + 2 = 17$, $3 . 5 + 4 = 19$, $3 . 5 + 8 = 23$.

Gilt in der Formel für q das negative Zeichen, nimmt man also $q = p - 2^n$, so muss, damit q positiv bleibe, $2^n < p$ und wegen der vorstehenden Bedingung $p - 2^n \leqq p - p_r^2$, also $2^n \geqq p - p_r^2$ sein. Hieraus folgt, dass, wenn zwischen den Werthen $p - p_r^2$ und p eine oder mehrere Potenzen von 2 liegen, jede derselben, wenn sie für 2^n genommen wird, in der Formel $q = p - 2^n$ eine Primzahl liefert, welche $> p_r$ ist, welche jedoch ausnahmsweise $= 1$ werden kann. Beispielsweise ist für $p = 3 . 5 . 7 = 105$, also $p - p_r^2 = 105 - 49 = 56$ und, da zwischen 56 und 105 die Potenz $2^6 = 64$ liegt; so ist $q = 105 - 64 = 41$ eine Primzahl > 7. Nimmt man $p = 3 . 5^2 . 7 = 525$, also $p - p_r^2 = 525 - 49 = 476$; so liegt zwischen 476 und 525 die Potenz $2^9 = 512$, folglich ist $q = 525 - 512 = 13$ eine Primzahl > 7.

Wenn $2^n > p$ wird, setzen wir $q = 2^n - p$. Die obige Bedingung verlangt dann $2^n - p \leqq p_r^2$ oder $2^n \leqq p + p_r^2$. Wenn hiernach

zwischen p und $p + p_r^2$ eine Potenz von 2 liegt, ist $q = 2^n - p$ eine Primzahl $> p_r$. Diess ist z. B. für $p = 3 . 5 = 15$ der Fall, da zwischen 15 und $15 + 5^2 = 40$ die Potenzen $2^4 = 16$ und $2^5 = 32$ liegen. Danach ist $16 - 15 = 1$ und $32 - 15 = 17$ eine Primzahl, worin die erstere $= 1$, die andere aber > 5 ist. Für $p = 3 . 5 . 7 = 105$, $105 + 49 = 154$ liegt zwischen 105 und 154 die Potenz $2^7 = 128$, und demzufolge ist $128 - 105 = 23$ eine Primzahl > 7.

Indem wir die Form $q = p + 2^n$ auf sich beruhen lassen, indem dieselbe nur für die kleinste Reihe von Primzahlen brauchbar ist, erfordert die Primzahl

$$q = p - 2^n, \quad \text{dass} \quad 2^n \geqq p - p_r^2 < p$$
$$q = 2^n - p, \quad \text{dass} \quad 2^n > p \qquad \leqq p + p_r^2$$

sei. Eine dieser beiden Bedingungen wird sicher erfüllt, wenn zwischen $p - p_1^2$ und $p + p_1^2$ eine Potenz von 2 liegt. Der gefundene Satz lautet hiernach: wenn zwischen $p - p_1^2$ und $p + p_1^2$ eine Potenz von 2 oder, wenn zwischen $\frac{log\,(p-p_r^2)}{log\,2}$ und $\frac{log\,(p+p_r^2)}{log\,2}$ eine ganze Zahl n liegt; so ist $p - 2^n$ eine positive oder negative Primzahl.

9) Wenn p_r eine Primzahl ist; so hat das Produkt aller unpaaren Zahlen bis hinauf zu p_r die Form $P = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{r-1}^{\alpha_{r-1}} p_r$, worin $p_1, p_2, \ldots p_r$ die vollständige Reihe aller Primzahlen bis p_r darstellt.

Dass in allen Fällen, wo P ein Produkt aus Potenzen aller Primzahlen $p_1, p_2 \ldots p_r$ ist, $P \mp 2^n$ mit beliebigem Werthe von n eine Zahl darstellt, welche aus lauter Primfaktoren $> p_r$ besteht (welche jedoch für das negative Zeichen ausnahmsweise $= 1$ werden kann), ist schon in Nr. 1 erwähnt: wir haben also in dieser Formel den Ausdruck für eine Zahl, welche aus lauter Primfaktoren besteht, die über einer gegebenen Grenze p_r liegen. Wenn übrigens die Bedingung aus voriger Nummer erfüllt ist, ist $P \mp 2^n$ selbst eine Primzahl, welche über der gegebenen Grenze liegt.

Wenn, wie früher, $p = p_1 p_2 \ldots p_r$ gesetzt wird; so ist $P = qp$, worin q ein aus beliebig vielen der Primzahlen $p_1, p_2, \ldots p_r$ oder deren Potenzen zusammengesetzter Faktor ist. Liegt also eine Potenz 2^n von 2 irgend einem solchen Produkte von p so nahe, dass ihr Abstand den Werth von p_r^2 nicht überschreitet; so ist $P - 2^n$ eine positive oder negative Primzahl.

10) Wir erweitern jetzt die vorstehende Betrachtung, indem wir unter $P = p_{\alpha_1}^{\alpha_1} p_{\alpha_2}^{\alpha_2} \ldots$ das Produkt beliebiger Potenzen beliebig vieler Primzahlen $p_{\alpha_1}, p_{\alpha_2}, \ldots$ aus der Reihe $p_1, p_2, \ldots p_r$ unter $Q = 2^n p_{\beta_1}^{\beta_1} p_{\beta_2}^{\beta_2} \ldots$ das Produkt einer Potenz von 2 und beliebigen Potenzen aller übrigen Primzahlen aus der Reihe $p_1, p_2, \ldots p_r$ verstehen und ausbedingen, dass alle Exponenten $\alpha_1, \alpha_2, \ldots \beta_1, \beta_2, \ldots$ und $n \geq 1$ seien. Jetzt ist die Zahl $q = P \mp Q$ entweder eine Primzahl oder sie besteht aus lauter Primfaktoren, welche $> p_r$ sind. Ganz derselbe

Schluss wie in Nr. 8 führt zu dem Satze, dass q eine Primzahl ist, wenn sie $\leq p_r^2$ ist. Diese Bedingung erfordert, wenn in q das positive Zeichen gilt, $P + Q \leq p_r^2$ also $Q \leq p_1^2 - P$, und wenn das negative Zeichen gilt, $P - Q \leq p_r^2$, also, falls $P > Q$ ist, $Q \geq P - p_r^2$ und, falls $P < Q$ ist, $Q - P \leq p_r^2$, mithin $Q \leq P + p_r^2$.

Nimmt man z. B. $p_r = 11$, $P = 5 \cdot 7 = 35$; so fragt es sich im ersten Falle, ob es unterhalb $11^2 - 5 \cdot 7 = 86$ eine Zahl von der Form $2^{\alpha} 3^{\beta_1} 11^{\beta_2}$ giebt. Da in der That $2 \cdot 3 \cdot 11 = 66 < 86$ ist; so ist $35 + 66 = 101$ eine Primzahl.

Der zweite Fall, in welchem das negative Zeichen gilt, enthält den Satz: Wenn zwischen $P - p_r^2$ und $P + p_r^2$ eine Zahl von der Form Q liegt, welche sich um mehr als eine Einheit von P unterscheidet; so ist $P - Q$ eine positive oder negative Primzahl, welche $> p_r$ ist. Nimmt man z. B. $p_r = 11$, $P = 5 \cdot 7 \cdot 11 = 385$; so liegen zwischen $385 - 11^2 = 264$ und $385 + 11^2 = 506$ mehrere Zahlen von der Form Q, nämlich $2^7 \cdot 3 = 384$, $2^5 \cdot 3^2 = 288$, $2^4 \cdot 3^3 = 432$, $2^2 \cdot 3^4 = 324$, $2 \cdot 3^5 = 486$, demzufolge sind alle nachstehenden Zahlen $385 - 384 = 1$, $385 - 288 = 97$, $385 - 432 = -47$, $385 - 324 = 61$, $385 - 486 = -101$ Primzahlen, welche mit Ausnahme der Zahl 1 grösser als 11 sind.

Man kann diese beiden Sätze auch so formuliren: Wenn die Summe zweier Zahlen von der Form P und Q kleiner als p_r^2 ist; so ist sie eine Primzahl. Wenn die absolute Differenz zweier solchen Zahlen kleiner als p_r^2 jedoch grösser als 1 ist; so ist sie eine Primzahl. Ist also, allgemein, nach absolutem Werthe $P \mp Q < p_r^2$ und > 1; so ist $P \mp Q$ eine Primzahl, grösser als p_r. So ist im ersten Beispiele $35 + 66 = 101 < 11^2$, folglich 101 eine Primzahl. Im zweiten Beispiele ist $385 - 288 = 97 < 11^2$, mithin 97 eine Primzahl, auch ist $385 - 432 = -47$ und $47 < 11^2$, mithin 47 eine Primzahl.

Ob eine der vorstehenden ähnliche Formel für eine Primzahl bereits aufgestellt worden, ist mir nicht bekannt.

11) Dieselbe Betrachtung wie in Nr. 8 lehrt, dass, wenn p_r^x die niedrigste Potenz von p_r ist, welche den Betrag $P \mp Q$ übersteigt, die Zahl $P \mp Q$ (insofern sie nicht $= \mp 1$ ist) höchstens aus $x - 1$ Primfaktoren bestehen kann, welche sämmtlich $> p_r$ sind. So ist z. B. für $p_r = 11$, wenn man $P = 5 \cdot 7 \cdot 11 = 385$ und $Q = 2^8 \cdot 9 = 2304$ setzt, die niedrigste Potenz von 11, welche über $2304 - 385 = 1919$ liegt, die 4-te. Danach kann die Zahl 1919 höchstens $4 - 1 = 3$ Primfaktoren enthalten, welche sämmtlich > 11 sind: sie ist in der That $= 19 \cdot 101$. Die niedrigste über $2304 + 385 = 2689$ liegende Potenz von 11 ist ebenfalls die 4-te, folglich kann auch 2689 höchstens aus 3 Primfaktoren > 11 bestehen: sie besteht in der That nur aus einem solchen Faktor; denn sie ist selbst eine Primzahl.

V. Zur allgemeinen Zahlentheorie.

§. 17. Die polyplexen Wurzeln einer Gleichung und die polyplexe Zahl überhaupt.

1) Die Auflösung der Gleichung $x^p = 1$, welche die Grundlage der Kreistheilung bildet, sowie überhaupt die Auflösung der algebraischen und transzendenten Gleichungen nach den in der heutigen Analysis gebräuchlichen Methoden stützt sich auf das Wesen der komplexen Grössen, von welchen die reellen Grössen als ein spezieller Fall erscheinen. Komplex heisst eine Grösse, insofern sie als Summe eines reellen und eines imaginären Gliedes in der Form $a + b\,i$, also überhaupt als ein durch das Additions- oder das Anreihungsgesetz gebildetes Aggregat von Theilen oder Gliedern aufgefasst wird. Wird eine Grösse als eine nach dem Multiplikations- oder dem Verhältnissgesetze gebildete Grösse oder als ein Verhältniss zur Einheit oder als ein Produkt von Faktoren, also in der Gestalt $a\,b\,c\,\ldots$ aufgefasst; so erscheint sie, wenn alle Faktoren durch unausgesetzte Anwendung einunddesselben Verhältnissgesetzes, also durch wiederholte Multiplikation der Einheit mit demselben Faktor oder mit der Basis ε gedacht werden, wenn also $a = 1\,.\,\varepsilon\,\varepsilon\,\varepsilon\,\ldots = \varepsilon^\alpha$, $b = \varepsilon^\beta$, $c = \varepsilon^\gamma$ etc. gesetzt wird, in derselben Form $\varepsilon^\alpha\,\varepsilon^\beta\,\varepsilon^\gamma\,\ldots = \varepsilon^{\alpha+\beta+\gamma+\cdots} = \varepsilon^\varphi$ als eine Potenz der Basis ε. Insofern es sich um die Erzeugung einer sekundären Verhältnissgrösse, nämlich einer solchen handelt, welche einen komplexen Werth hat; so nimmt die Basis ε den Werth einer Potenz von -1, oder auch den ihr äquivalenten Werth einer imaginären Potenz der Basis e der natürlichen Logarithmen an, indem man $(-1)^n = e^{n\pi i}$ hat. Hiernach ergiebt sich für eine komplexe Grösse $a + b\,i$, deren absolute Quantität $\sqrt{a^2 + b^2}$ gleich der Einheit ist, der äquivalente Ausdruck $(-1)^{\frac{\varphi}{\pi}}$ oder $e^{\varphi i}$.

Während die arithmetische Anreihung dem geometrischen Fortschritte, insbesondere die Anreihung einer reellen Grösse an eine reelle dem Fortschritte im Sinne der Grundrichtung, die Anreihung einer imaginären Grösse an eine reelle aber dem Fortschritte in der Seitenrichtung oder dem Austritte aus der Grundrichtung entspricht, entspricht die primäre arithmetische Verhältnissbildung oder die Multiplikation einer positiv reellen Zahl mit einer positiv reellen Zahl einer geometrischen gleichmässigen Expansion einer Grösse nach allen Seiten in einem bestimmten Maasse, und die sekundäre arithmetische Verhältnissbildung oder die Multiplikation einer reellen Zahl mit einer sekundären Verhältnisszahl $e^{\varphi i}$ einer geometrischen Drehung des Multiplikands um den Winkel φ in der Grundebene oder einer Richtungsänderung. Da hiernach der Faktor $e^{\varphi i}$ die Richtung des damit behafteten reellen Faktors bedingt; so trägt er den Namen des Richtungskoeffizienten. Immer bleibt sowohl in dem geometrischen, als auch in dem arithmetischen, sekundären Multiplikationsprozesse die Voraussetzung maassgebend, dass dieser Prozess, nämlich geometrisch die Drehung einer Linie stets in einunderselben bestimmten Grundebene vor sich gehe, und dass ebenso die arithmetische sekundäre Verhältnissbildung eine Veränderung in dem gemeinsamen Be-

reiche aller möglichen reellen und imaginären oder aller komplexen Grössen sei: denn nur unter Innehaltung dieser geometrischen Grundebene oder dieser arithmetischen Grundgattung behalten die durch fortgesetzte Drehung, resp. sekundäre Multiplikation entstehenden Grössen unter sich und zu der Grundeinheit diejenigen Relationen, auf welchen ihre Theorie beruhet. Verliesse die Grösse a nach der ersten Drehung vermittelst der Multiplikation mit $e^{\varphi i}$, wodurch sie den Werth $a\,e^{\varphi i}$ angenommen hat, bei der zweiten Drehung vermittelst der Multiplikation mit $e^{\psi i}$ die Grundebene, läge also $a\,e^{\varphi i}\,e^{\psi i}$ nicht in der Grundebene; so entspräche der arithmetische Ausdruck $a\,e^{(\varphi+\psi)i}$ durchaus nicht dem geometrischen Werthe der entstehenden Linie: denn offenbar ist alsdann $\varphi + \psi$ nicht der Neigungswinkel dieser Linie gegen die Grundgrösse a, und die Summe der beiden Neigungswinkel φ und ψ, unter welchen sich resp. die zuerst erzeugte Linie gegen a und die zuletzt erzeugte Linie gegen die vorhergehende neigt, ist nun nicht mehr gleich dem Neigungswinkel der letzten gegen die erste, und damit ist die Analogie zwischen diesen arithmetischen und den entsprechenden geometrischen Grössen aufgehoben.

Eine tertiäre Multiplikation oder eine Verhältnissoperation, welche aus der Grundgattung der komplexen Grössen hinaus führt und demgemäss der geometrischen Wälzung aller in der Grundebene möglichen Grössen um die Grundaxe entspricht; muss von der sekundären Verhältnissbildung offenbar ebenso unabhängig sein, wie die sekundäre Verhältnissbildung von der primären und wie der imaginäre Fortschritt von dem reellen es ist. Eine solche Operation kann durch einen sekundären Richtungskoeffizienten $e^{\varphi i}$ schlechterdings nicht vertreten werden; vielmehr muss der diesen Vorgang anzeigende Koeffizient in seinem Exponenten unbedingt ein ganz neues Symbol sein, welches die neue und vollkommen selbstständige Veränderung anzeigt: es ist Diess der Koeffizient $(\div 1)^{\frac{\psi}{\pi}} = e^{\psi i_1}$, welchen ich den Inklinationskoeffizienten genannt habe, während $e^{\varphi i}$ als der Deklinationskoeffizient erscheint. Unter i_1 verstehe ich den Ausdruck $\sqrt{\div 1}$, nämlich die Quadratwurzel aus der Grösse $\div 1$, worin das Symbol $\div$, welches wir cominus nennen, als Faktor $\div 1$ das Resultat der halben Umwälzung um die Grundaxe anzeigt, gleichwie der Faktor -1 das Resultat der halben Umdrehung um den Nullpunkt in der Grundebene vertritt.

Hiernach entspricht der Faktor $ii_1 = \sqrt{-1}\ \sqrt{\div 1}$ dem tertiären Fortschritte im Raume in der Höhenrichtung aus der Grundebene hinaus, und man erhält durch das Produkt des Deklinations- und Inklinationskoeffizienten die überkomplexe oder triplexe Grösse

$$\begin{aligned}(-1)^{\frac{\varphi}{\pi}}\ (\div 1)^{\frac{\psi}{\pi}} &= e^{\varphi i}\,e^{\psi i_1} = a + bi + cii_1\\ &= \cos\varphi + \sin\varphi\,\cos\psi i + \sin\varphi\,\sin\psi\, ii_1\end{aligned}$$

welche geometrisch, wenn es sich um Linien handelt, eine Linie im Raume von der Länge der Einheit einmal als Multiplikationsresultat der Dekli-

nation φ und Inklination ψ und einmal als Additionsresultat der drei neutralen Glieder a, $b\,i$ und $c\,i\,i_1$ darstellt.

Die reellen, die komplexen oder eigentlich duplexen und die überkomplexen oder eigentlich triplexen Grössen sind die Grössen resp. des eindimensionalen, des zweidimensionalen und des dreidimensionalen Grössengebietes, von welchen ich in der Schrift über das Verhältniss der Arithmetik zur Geometrie, im Situationskalkul, in der Schrift über die polydimensionalen Grössen, in den Naturgesetzen, in dem Buche über die Welt nach menschlicher Auffassung und über die Grundlagen der Wissenschaft gehandelt habe. Das allgemeine Grössengebiet von unendlich viel Dimensionen hebt sich in unendlicher Stufenleiter über jene ersten Gebiete hinaus, sodass generell n-dimensionale Grössen in Betracht kommen. Jedes höhere Gebiet erfordert als Basis des ihm eigenen Verhältnissgesetzes ein besonderes Symbol in der Form —, ÷, ⁝ u. s. w. Da jedes höhere Gebiet ein allgemeineres ist, welchem alle niedrigeren Gebiete als untergeordnete Spezialitäten angehören; so ist es unmöglich, dass die Gesetze eines Gebietes die Gesetze eines höheren Gebietes umfassen. Nach aller Logik schliesst das Allgemeine das Besondere ein, wogegen das Besondere das Allgemeine ausschliesst. Die speziellen Grössenbeziehungen, welche für ein Gebiet gelten, gelten gewiss für jedes niedrigere Gebiet, sie können jedoch nicht für ein höheres Gebiet gelten, d. h. sie enthalten vollständig alle Gesetze des niedrigeren Gebietes, sie erschöpfen aber nicht die Gesetze des höheren Gebietes; die Gesetze des niedrigeren Gebietes sind, als Spezialitäten der Gesetze des höheren Gebietes, von diesen abhängig, die Gesetze des höheren Gebietes dagegen sind, als Verallgemeinerungen der Gesetze des niedrigeren Gebietes, von diesen unabhängig. Hiermit trete ich in entschiedene Opposition gegen die Ansicht, dass die heutigen Gesetze der Algebra und Zahlentheorie, welche sich auf komplexe Zahlen stützen, die allgemeinen Grössengesetze enthalten, trotzdem diese Ansicht an einem Ausspruche des grossen Mathematikers Gauss eine autoritative Stütze gefunden hat. Die nachstehenden Betrachtungen über die Kugeltheilung werden eine Bestätigung der aufgestellten Behauptungen bringen.

2) Die Sätze, dass eine algebraische Gleichung n-ten Grades n Wurzeln habe und dass sich eine ganze rationale Funktion n-ten Grades in n lineare Faktoren nach der Formel

$$x^n + a_1\,x^{n-1} + a_2\,x^{n-2} + \ldots + a_{n-1}\,x + a_n$$
$$= (x - x_1)\,(x - x_2)\,(x - x_3)\,\ldots\,(x - x_n)$$

zerlegen lasse, sind nur für das zweidimensionale Grössengebiet, nämlich nur für komplexe (und reelle) Zahlen richtig, für höhere Gebiete, also allgemein oder für das Zahlengebiet schlechthin sind sie falsch.

Wäre das Polynom auf der linken Seite, welches wir mit $F(x)$ bezeichnen, für jeden beliebigen Werth von x dem Produkte auf der rechten Seite, welches wir mit $P(x)$ bezeichnen, gleich; so müssten beide identisch sein: entwickelt man also $P(x)$ durch Ausführung der Multiplikationen in das Polynom

$$x^n - (x_1 + x_2 + \ldots)\, x^{n-1} + (x_1 x_2 + x_2 x_3 + \ldots)\, x^{n-2} - (x_1 x_2 x_3 + x_2 x_3 x_4 + \ldots)\, x^{n-3} + \ldots (-1)^n (x_1 x_2 \ldots x_n)$$

so müssten die Koeffizienten der in gleiche Potenzen von x multiplizirten Glieder einander gleich sein, die n Grössen $x_1, x_2, \ldots x_n$ müssten also den n Gleichungen

$$x_1 + x_2 + \ldots = -a_1 \qquad x_1 x_2 + x_2 x_3 + \ldots = a_2$$
$$x_1 x_2 x_3 + x_2 x_3 x_4 + \ldots = -a_3$$

u. s. w. genügen, und wenn sie Diess thäten, bestände die erwartete Identität. Nun würden n Gleichungen zur Bestimmung der n Unbekannten $x_1, x_2, \ldots$ ausreichen, wenn die zu lösende Finalgleichung für die darin erscheinende einzige Unbekannte eine Gleichung ersten Grades wäre, weil nur eine solche einen einzigen Werth für die Unbekannte zulässt. Die Elimination der $n - 1$ Unbekannten $x_2, x_3, \ldots x_n$ ergiebt aber selbst nach Ausscheidung der durch das Eliminationsverfahren etwa eingeführten fremden Faktoren (vgl. meine Auflösung der algebraischen und transzendenten Gleichungen mit einer und mehreren Unbekannten, §. 12) eine Restgleichung höheren Grades, welche für x_1 mehr als einen Werth zulässt. Jedem dieser Werthe von x_1 entsprechen dann gewisse Werthe von $x_2, x_3, \ldots x_n$, man erhält also mehr als eine Auflösung oder mehrere Systeme der Grössen $x_1, x_2, \ldots x_n$, welche der Forderung genügen. Dass alle diese Systeme von der Art seien, dass darin nur n ganz bestimmte Werthe der Unbekannten erscheinen, oder dass bei dem Übergange von dem einen Systeme zu dem andern die Werthe für $x_1, x_2, \ldots x_n$ nur die Stelle wechseln, oder dass die Auflösungen, welche die Restgleichung für x_1 ergiebt, nur die eben erwähnten n Werthe liefern, sodass jeder andere Werth für x_1 nur ein zulässiger Werth von einer der übrigen Unbekannten sei, ist nicht generell, sondern nur unter der Voraussetzung komplexer Zahlen nachweisbar und findet auch, wie wir sogleich zeigen werden, nicht allgemein, sondern nur für komplexe Zahlen statt.

Giebt es nun aber verschiedene Systeme von Auflösungen für $x_1, x_2, \ldots x_n$; so kann ein einzelnes derselben nicht die Identität zwischen $F(x)$ und $P(x)$ begründen. In der That, müsste in diesem Falle, wo $x_1', x_2', \ldots x_n'$ ein erstes, und $x_1'', x_2'', \ldots x_n''$ ein zweites System von Auflösungen ist,

$$\begin{aligned} F(x) &= x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots \\ &= (x - x_1')(x - x_2')(x - x_3') \ldots = P'(x) \\ &= (x - x_1'')(x - x_2'')(x - x_3'') \ldots = P''(x) \end{aligned}$$

sein. Hiernach wird, wenn man für x irgend einen beliebigen Werth entweder aus dem Systeme $x_1', x_2', \ldots$ oder aus dem Systeme $x_1'', x_2'', \ldots$ substituirt, das betreffende Produkt $P'(x)$ oder $P''(x)$, also auch das Polynom $F(x)$ gleich null werden, es wird aber das andere Produkt nicht gleich null werden, wenn der für x substituirte Werth keinem der darin erscheinenden Werthe für $x_1, x_2, \ldots$ gleich ist. Wegen des betreffenden Produktes müsste also $F(x)$ gleich null und wegen des anderen Produktes müsste $F(x)$ verschieden von null sein, was offenbar absurd ist. Das

Produkt aus n binomischen Faktoren kann daher nicht mit einem Polynome vom n-ten Grade identisch, also auch nicht für jeden beliebigen Werth von x diesem Polynome gleich sein.

Manche Mathematiker halten es zwar für möglich, dass ein Produkt verschwinde, ohne dass einer seiner Faktoren verschwindet, was, wenn es wirklich stattfände, die Möglichkeit der Identität zwischen $F(x)$ und $P(x)$ noch offen erhielte: allein diese Annahme enthält einen krassen Widerspruch gegen die Grundanschauungen und Grundgesetze der Mathematik, da eine wiederholte Verhältnissbildung oder Multiplikation, welche prinzipiell die absolute Quantität des Multiplikands in einem bestimmten Verhältnisse vergrössert oder verkleinert und seine Richtung ohne Beeinflussung der Quantität um einen bestimmten Winkelbetrag, der dem Exponenten des Richtungskoeffizienten proportional ist, ändert, nur dadurch den Nullwerth herbeiführen kann, dass sie die Quantität vernichtet, der letztere Effekt aber nur durch einen Faktor herbeigeführt werden kann, welcher eine Theilung nach einem unendlich grossen Verhältnisse verlangt, welcher also selbst den Nullwerth in der Form $\frac{1}{\infty}\varrho$, worin ϱ einen beliebigen Richtungskoeffizienten bezeichnet, darstellt.

3) Durch mehrmalige ganze Umdrehungen um den Nullpunkt und durch mehrmalige ganze Umwälzungen um die Grundaxe nimmt eine Grösse a immer wieder ihren ursprünglichen Werth an, d. h. das Endresultat des Multiplikationsprozesses, welcher an der Grösse a mit dem Deklinationskoeffizienten $e^{2r\pi i}$ und mit dem Inklinationskoeffizienten $e^{2s\pi i_1}$, worin r und s beliebige ganze Zahlen sind, vollzogen wird, deckt die ursprüngliche Grösse a. Eine solche Deckung der Endresultate zweier Prozesse heisst Gleichheit, nicht Identität, man hat also, wenn man unter der ursprünglichen Grösse a den fundamentalen Werth $ae^{0i}e^{0i_1}$ versteht, die Gleichung

$$a = ae^{2r\pi i}\, e^{2s\pi i_1} = (-1)^{2r}(\div 1)^{2s}a$$

welche nicht als eine Identität aufgefasst werden darf, indem die eine dieser beiden Grössen die Deklination $2r\pi$ und die Inklination $2s\pi$, die andere dagegen die Deklination 0 und die Inklination 0 hat. Die n-te Wurzel der Grösse a ist daher, wenn man für a jeden beliebigen der ihr gleichen, wiewohl nicht identischen Werth zulässt und unter α die n-te Wurzel des absoluten Werthes oder der reinen Quantität von a versteht,

$$\sqrt[n]{a} = \alpha e^{\frac{2r\pi i}{n}} e^{\frac{2s\pi i_1}{n}} = (-1)^{\frac{2r}{n}}(\div 1)^{\frac{2s}{n}}\alpha$$

Nimmt man für a die Einheit 1; so ergiebt sich, da der Faktor α auf der rechten Seite $= 1$ ist,

$$\sqrt[n]{1} = e^{\frac{2r\pi i}{n}} e^{\frac{2s\pi i_1}{n}} = (-1)^{\frac{2r}{n}}(\div 1)^{\frac{2s}{n}}$$

$$\sqrt[n]{a} = \alpha\sqrt[n]{1}$$

Die n-te Wurzel einer Grösse a hat also, wenn n eine reelle ganze Zahl ist, n^2 verschiedene Werthe, wenn man triplexe Zahlen zulässt. Diese Werthe ergeben sich, indem man r und s zwischen den ganzen Zahlen 0, 1, 2, ... $(n-1)$ oder 1, 2, 3, ... n variiren lässt. Wir heben mit Nachdruck hervor, dass die Vieldeutigkeit der Wurzel aus a ihren Grund durchaus nicht in einer Unbestimmtheit des Radikationsprozesses, sondern lediglich in der Vielwerthigkeit der Grösse a selbst hat. Ist a nach Quantität, Deklination und Inklination in der Form $a e^{\alpha i} e^{\beta i_1}$ fest gegeben; so hat die n-te Wurzel nur den einzigen Werth $a^{\frac{\alpha}{n} i} e^{\frac{\beta}{n} i_1} \sqrt[n]{a}$. Die vieldeutige Wurzel ist also die bestimmte Wurzel aus einer vielwerthigen Grösse.

Von den n^2 Wurzeln decken die n Werthe von der Deklination null nämlich $e^{0i\,0i_1}, e^{0i\,\frac{2\pi i_1}{n}}, e^{0i\,\frac{4\pi i_1}{n}} \ldots e^{0i\,\frac{2(n-1)\pi i_1}{n}}$ die positiv reelle Einheit 1. Wenn man dieselben wie gleiche Grössen ansieht; so verbleiben $n^2 - n + 1$ Werthe, welche sich nicht decken, wenn n unpaar ist. Für ein paares n kommen auch n Werthe von der Deklination π vor, welche die negative Einheit -1 decken, sodass alsdann die Anzahl der sich deckenden Wurzeln $n^2 - 2n + 2$ ist.

Die Anzahl der verschiedenen Werthe der Wurzel aus einer gegebenen Grösse a hängt nicht allein von dem Wurzelgrade n, sondern auch von der Dimensität des Grössengebietes ab, in welchem man beschlossen hat, sich zu bewegen. Operirt man im eindimensionalen Gebiete der absoluten Grössen, welches keine Richtungskoeffizienten, sondern nur reine Quantitäten kennt; so hat die n-te Wurzel aus a nur einen einzigen Werth $\sqrt[n]{a} = a$. Operirt man im zweidimensionalen Gebiete der komplexen Grössen; so hat die n-te Wurzel aus a überhaupt n verschiedene Werthe, wovon ein einziger positiv reell ist. Operirt man im dreidimensionalen Gebiete der triplexen Grössen; so hat die n-te Wurzel aus a überhaupt n^2 verschiedene Werthe, wovon die n Werthe

$$a e, \quad a e^{\frac{2\pi}{n} i}, \quad a e^{\frac{2.2\pi}{n} i}, \quad \ldots \quad a e^{\frac{2(n-1)\pi}{n} i}$$

dem zweidimensionalen Gebiete angehören, also bis auf einen reellen Werth komplex sind. Operirt man im vierdimensionalen Gebiete der quadruplexen Grössen; so hat die n-te Wurzel aus a überhaupt n^3 verschiedene Werthe, von der Form $a e^{\frac{2r\pi i}{n}} e^{\frac{2s\pi i_1}{n}} e^{\frac{2t\pi i_2}{n}}$, wovon n^2 Werthe dem dreidimensionalen, n Werthe dem zweidimensionalen und 1 Werth dem eindimensionalen Gebiete angehören. (Einige der dem höheren Gebiete zugezählten Werthe fallen in die Basis dieses Gebietes, welche zugleich das nächst niedrigere Gebiet darstellt: allein, nach ihrem vollständigen Richtungskoeffizienten gehören sie doch dem höheren Gebiete an. Die in die positive Grundaxe, sowie die bei paarem n in die negative Grundaxe fallenden Werthe decken sich untereinander, ohne doch nach ihrem Richtungskoeffizienten identisch zu sein).

4) Schon in der Einleitung der Beiträge zu der Theorie der Gleichungen habe ich angeführt, dass auch die Vielwerthigkeit der Wurzel einer

Gleichung $F(x) = 0$ lediglich auf der Vieldeutigkeit ihrer Koeffizienten beruht. Eine Gleichung n-ten Grades mit fest gegebenen Koeffizienten kann nur eine einzige Wurzel haben, d. h. nur ein einziger Werth von x vermag durch seine Substitution die Gleichung vollständig zu erfüllen. Wenn wir jetzt die dreidimensionalen Zahlen in Betracht ziehen; so hat nach dem Vorstehenden die Gleichung $x^n - 1 = 0$ im Ganzen n^2 verschiedene Wurzeln, da jeder der vorstehenden Werthe von $\sqrt[n]{1}$ ihr genügt. Diese Erfüllung der gegebenen Gleichung durch n^2 verschiedene Werthe von x begründet sich eben dadurch, dass man unter dem bekannten Gliede 1 nicht einen einzigen, sondern n^2 nicht identische Werthe, nämlich die Werthe $e^{2r\pi i} e^{2s\pi i_1}$ versteht, welche sich durch eine Variation des r und s in der Reihe der Zahlen $0, 1, 2, \ldots (n-1)$ ergeben. Wenn man aber in der gegebenen Gleichung $x^n = 1$ den Werth von 1 oder den ihm gleich gesetzten Werth von x^n in der bezeichneten Weise unbestimmt lässt, ist es begreiflich, dass von keinem bestimmten oder einzigen Werthe von x selbst die Rede sein kann. Während die verschiedenen Werthe von 0 sich nur um ganze Umdrehungen und Umwälzungen unterscheiden, also sich geometrisch decken, unterscheiden sich die n^2 Werthe $e^{\frac{2r\pi i}{n}} e^{\frac{2s\pi i_1}{n}}$ der Wurzel x durch Theile ganzer Umdrehungen und Umwälzungen, decken sich also nicht oder sind im eigentlichen Sinne des Wortes ungleich; die Vielheit dieser ungleichen Werthe von x ist aber die unmittelbare Folge der Unbestimmtheit der Zahl 1. Bewegt man sich auf eindimensionalem Gebiete; so ist 1 nicht mehr vieldeutig, und daher hat dann auch $\sqrt[n]{1}$ nur den einzigen Werth 1. Auf zweidimensionalem Gebiete kommen für 1 nur die n Werthe $e^{2r\pi i}$ und daher für $\sqrt[n]{1}$ nur n ungleiche, sich nicht deckende Werthe in Betracht. Auf dreidimensionalem Gebiete liefern die erwähnten n^2 Werthe von 1 ebenso viel ungleiche Werthe für $\sqrt[n]{1}$.

Hieraus geht hervor, dass die Gleichung

$$(x - x_1)(x - x_2) \ldots (x - x_n) = 0$$

deren linke Seite aus n linearen Faktoren besteht, nicht der Vertreter der Gleichung $x^n - 1 = 0$ sein kann, da jene nur durch n Werthe, diese aber durch n^2 Werthe von x erfüllt wird. Eine Gleichung $(x - x_1)(x - x_2) \ldots (x - x_{n^2}) = 0$, deren linke Seite n^2 Faktoren hat, kann aber, selbst wenn sie durch jede Wurzel der Gleichung $x^n - 1 = 0$ erfüllt wird, ebenfalls nicht mit dieser Gleichung identisch sein, da ein Polynom vom n^2-ten Grade nimmermehr einem Polynom vom n-ten Grade für jeden beliebigen Werth von x gleich und daher mit demselben nicht identisch sein kann. Es bleibt nur der mögliche Fall übrig, dass sich der Ausdruck $x^n - 1$ auf mehr als eine, nämlich auf n verschiedene Weisen in ein Produkt von n Faktoren zerlegen lasse. Dieser Fall entspricht der Wirklichkeit, wenn nachgewiesen wird, dass die Koeffizienten des Polynoms, welches sich durch die Ausführung der Multiplikation jener n binomischen Faktoren $(x - x_1)$, $(x - x_2)$, ... ergiebt, den Koeffizienten des Ausdruckes $x^n - 1$ nicht nur für ein bestimmtes System von n Ein-

heitswurzeln, sondern für n verschiedene solche Systeme, die keine Wurzel miteinander gemein haben, gleich werden, dass also alle symmetrischen Funktionen aus den n einem solchen Systeme angehörigen Wurzeln mit Ausnahme der höchsten Funktion den Nullwerth annehmen, während die aus einem einzigen Gliede bestehende höchste symmetrische Funktion $x_1 x_2 \ldots x_n = (-1)^{n-1}$ wird.

Um Diess zu zeigen, stellen wir die n^2 Einheitswurzeln vom Grade n, welche sich durch die Variation von r und s zwischen den Werthen 0, 1, 2, ... $n-1$ aus dem Ausdrucke $e^{\frac{2r\pi i}{n}} e^{\frac{2s\pi i_1}{n}}$ ergeben, in n Gruppen von je n Wurzeln nach der einen oder nach der anderen der beiden nachfolgenden Regeln zusammen. Die erste Regel stützt sich auf die Konstanz der Inklination in jeder Gruppe, wir nehmen also in derselben Gruppe diejenigen Wurzeln auf, worin s denselben Werth hat, während r von irgend einem Anfangswerthe r' an die Werthe r', $r'+1$, $r'+2$, ... $r'+n-1$ durchläuft. Die zweite Regel setzt eine gemeinschaftliche, aber gleichmässige Variation der Inklination und Deklination voraus, sodass in dieselbe Gruppe diejenigen Wurzeln gestellt werden, für welche das r und s zwei untereinander stehende Werthe der beiden Reihen

$$\begin{array}{cccccc} r' & r'+1 & r'+2 & \ldots & r'+n-1 \\ s' & s'+1 & s'+2 & \ldots & s'+n-1 \end{array}$$

besitzen, wobei man entweder die oberste oder die unterste Reihe, d. h. entweder das r' oder das s' für alle Gruppen gleich annimmt.

Setzen wir zur Abkürzung den Deklinationskoeffizienten, welcher dem n-ten Theile einer ganzen Umdrehung oder der kleinsten, resp. niedrigsten komplexen n-ten Einheitswurzel entspricht, $e^{\frac{2\pi i}{n}} = \alpha$, den Inklinationskoeffizienten, welcher dem n-ten Theile einer ganzen Umwälzung entspricht, $e^{\frac{2\pi i_1}{n}} = \beta$; so sind die Wurzeln der n Gruppen sowohl für die Zusammenstellung nach der ersten, als auch für die nach der zweiten Regel dargestellt durch die Horizontalreihen der Tafel

$$\begin{array}{cccccc} 1 & \gamma & \gamma^2 & \ldots & \gamma^{n-1} \\ \beta & \beta\gamma & \beta\gamma^2 & \ldots & \beta\gamma^{n-1} \\ \beta^2 & \beta^2\gamma & \beta^2\gamma^2 & \ldots & \beta^2\gamma^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta^{n-1} & \beta^{n-1}\gamma & \beta^{n-1}\gamma^2 & \ldots & \beta^{n-1}\gamma^{n-1} \end{array}$$

wenn man für die erste Regel $\gamma = \alpha$ und für die zweite Regel $\gamma = \alpha\beta$ setzt.

Weiter oben in §. 4 haben wir gezeigt, dass sich jede symmetrische Funktion aus zyklisch geordneten primitiven Gruppen zusammensetzt. Diese Gruppen haben nicht immer n Glieder: wenn n eine zusammengesetzte Zahl ist, können kürzere Gruppen vorkommen, deren Gliederzahlen den Faktoren von n entsprechen. Nach §. 4 Nr. 18 ist aber jede kürzere Primitivgruppe gleichwerthig mit einem aliquoten Theile einer n-gliedrigen Gruppe, welche bei der Fortsetzung ihr erstes Glied identisch wiedererzeugt. Betrachten wir nun irgend eine n-gliedrige, zyklisch ge-

ordnete Gruppe einer symmetrischen Funktion. Sind w_1, w_2, w_3, ... die Vertreter der Elemente und ist $w_1\ w_a\ w_b\ w_c$ das erste Glied der Gruppe; so ist die Gruppe dargestellt durch

$$w_1\ w_a\ w_b\ w_c + w_2\ w_{a+1}\ w_{b+1}\ w_{c+1} + \ldots + w_n\ w_{a+n}\ w_{b+n}\ w_{c+n}$$

wobei wir in den Reihen, welche das zweite Element w_a, das dritte Element w_b, das vierte Element w_c u. s. w. durchlaufen, sobald der Zeiger n erreicht ist, nicht auf den Zeiger 1 zurückspringen, sondern, weiter zählend, die gleichen Grössen w_{n+1}, w_{n+2}, ... dafür stehen lassen. Eine solche n-gliedrige Gruppe (selbst wenn sie keine Primitivgruppe, sondern nach §. 4 Nr. 18 das Vielfache einer solchen ist) stellt immer, wenn man für die Elemente w die entsprechenden Wurzeln einer Horizontalreihe der obigen Tafel setzt, eine geometrische Progression von der Form

$$A + A\gamma^r + A\gamma^{2r} + \ldots + A\gamma^{(n-1)r}$$

dar. Die Summe derselben hat nach der elementaren Formel den Faktor $\gamma^{nr} - 1$ und da γ^n in allen Fällen (mag man die Tafel nach der ersten, oder nach der zweiten Regel gebildet haben) den Werth 1 deckt; so ist dieser Faktor und mithin die in Rede stehende n-gliedrige zyklische Funktion gleich null. Weil aber eine zyklische Primitivgruppe, wenn sie weniger als n Glieder enthält, ein aliquoter Theil einer n-gliedrigen Funktion ist; so hat auch eine solche, also jede zyklische symmetrische Primitivgruppe den Nullwerth. Jede vollständige symmetrische Funktion besteht aus primitiven Gruppen, hat also den Nullwerth, wenn sie aus den n Einheitswurzeln einer Horizontalreihe der obigen Tafel gebildet ist. Nur die höchste Funktion von n Dimensionen macht eine Ausnahme; sie besteht aus dem einzigen Gliede $w_1\ w_2 \ldots w_n$, welches, jenachdem die Wurzeln w nach der ersten oder nach der zweiten Regel gebildet sind, den Werth

$$\beta^{m\,n}\ e^{(n-1)\pi i} \quad \text{oder} \quad \beta^{m\,n}\ e^{(n-1)\pi i}\ e^{(n-1)\pi i},$$

hat, welcher in beiden Fällen durch den Werth von $(-1)^{n-1}$ gedeckt wird.

Hiermit ist erwiesen, dass sich das Binom $x^n - 1$ in n triplexe Faktoren von der Form $x - w$ zerlegen lässt, und dass für w die n Einheitswurzeln gesetzt werden können, welche irgend eine Horizontalgruppe der obigen Tafel ausfüllen, einer Tafel, welche nach zwei verschiedenen Regeln (mit konstanter und mit variabeler Inklination) aufgestellt werden kann. Da die Tafel n Gruppen hat; so lässt sich das Binom $x^n - 1$ auf n verschiedene Weisen in n Faktoren zerlegen, und da mehrere Tafeln in Betracht kommen; so können die n Gruppen von je n Faktoren sogar innerhalb der Gesammttafel von n^2 Faktoren mehrfach variirt werden.

Im Bereiche der komplexen Zahlen existirt ein solches Gesetz der mehrfachen Zerlegbarkeit einer Funktion nicht; das vorstehende Gesetz charakterisirt die Gesetze des triplexen Gebietes als allgemeinere, höhere und eigenartige gegenüber denen des komplexen Gebietes.

Wenn man den Begriff der Potenzirung und Wurzelausziehung dahin erweitert, dass man nicht nach der ursprünglichen Auffassung eine Zusammensetzung aus identischen Faktoren, resp. eine Zerlegung in identische Faktoren, sondern nur eine Zusammensetzung aus gleichen

Faktoren, resp. eine Zerlegung in gleiche Faktoren verlangt, also das Produkt $a_1\ a_2\ a_3\ \ldots\ a_n = a^n$ setzt, wenn die Faktoren $a_1, a_2, a_3, \ldots$ gleiche Werthe haben, und umgekehrt sowohl a_1, als auch $a_2, a_3, \ldots$ für die Wurzel von b nimmt oder $= \sqrt[n]{b}$ setzt, insofern das Produkt $a_1\ a_2 \ldots a_n = b$ ist und $a_1, a_2, \ldots$ einander gleich sind; so kann man, wenn $x_1, x_2, \ldots x_{n^2}$ die n^2 triplexen Einheitswurzeln sind,

$$x^n - 1 = \sqrt[n]{(x - x_1)\ (x - x_2)\ \ldots\ (x - x_{n^2})}$$

setzen: denn das Produkt aus n^2 Faktoren unter dem Wurzelzeichen zerfällt in n einander gleiche Produkte von je n Faktoren.

Die vorstehende Rechnung hat uns gelehrt, dass die symmetrischen Funktionen der n Einheitswurzeln $1, \varrho, \varrho^2, \ldots \varrho^{n-1}$, worunter sich die reelle Wurzel 1 befindet, mit Ausnahme der höchsten gleich null sind. Von Wichtigkeit sind auch die symmetrischen Funktionen der $n-1$ nicht reellen Einheitswurzeln $\varrho, \varrho^2, \ldots \varrho^{n-1}$. Schliesst man von den obigen Horizontalreihen immer das erste Glied, welches die Einheit 1 deckt, aus; so ergiebt sich für irgend eine dieser Reihen als erste symmetrische Funktion der betreffenden $n - 1$ Wurzeln

$$\beta^m (\gamma + \gamma^2 + \gamma^3 + \ldots + \gamma^{n-1}) = -\beta^m = -1$$

weil nach dem Vorstehenden die symmetrische Funktion der n Wurzeln $1 + \gamma + \gamma^2 + \ldots + \gamma^{n-1} = 0$ ist.

Bezeichnet man die symmetrische Funktion aus n Elementen $w_1, w_2, w_3, \ldots w_n$ von 1, 2, $\ldots$ m Dimensionen resp. mit ${}^nf_1, {}^nf_2, \ldots {}^nf_m$ und die gleich hohen symmetrischen Funktionen aus den $n - 1$ Elementen $w_2, w_3, \ldots w_n$ resp. mit ${}^{n-1}f_1, {}^{n-1}f_2, \ldots {}^{n-1}f_m$; so ist offenbar allgemein ${}^nf_m = w_1\ {}^{n-1}f_{m-1} + {}^{n-1}f_m$. Kennt man also alle Funktionen ${}^nf$ und von den Funktionen ${}^{n-1}f$ die ersten $m - 1$; so ergiebt sich die nächst folgende durch die Beziehung ${}^{n-1}f_m = {}^nf_m - w_1\ {}^{n-1}f_{m-1}$. In dem vorliegenden Falle ist ${}^nf_1 = {}^nf_2 = {}^nf_3 = \ldots = {}^nf_{n-1} = 0$, ${}^nf_n = (-1)^{n-1}$, $w_1 = 1$, folglich ${}^{n-1}f_1 = -1$, ${}^{n-1}f_2 = 1$, ${}^{n-1}f_3 = -1$, überhaupt ${}^{n-1}f_m = (-1)^m$.

Hieraus geht hervor, dass für alle $n - 1$ Werthe von x, welche in der obigen Gruppe eine Horizontalreihe nach Ausschluss des ersten Gliedes bilden, die Gleichung

$$x^{n-1} + x^{n-2} + \ldots + x + 1 = 0$$

besteht.

5) Gehen wir jetzt von dem Binome $x^n - 1$ zu dem Polynome $F(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a^n$ über. Das Verfahren, welches dazu dient, die Zerlegung dieses Polynoms in n Faktoren von der Form $x - x_1, x - x_2, \ldots x - x_n$ zu bewirken, worin $x_1, x_2, \ldots x_n$ die n Wurzeln der Gleichung $F(x) = 0$ darstellen, führt nach meinen Beiträgen zur Lehre von den Gleichungen §. 15 gleichviel, ob n eine Primzahl ist oder nicht, zu der Erkenntniss, dass die Wurzel dieser Gleichung die allgemeine Form

$$x = b + \alpha b_1 + \beta b_2 + \gamma b_3 + \ldots + \omega b_{n-1}$$

hat, worin $\alpha, \beta, \gamma, \ldots \omega$ irgend welche der $n-1$ komplexen Einheitswurzeln vom Grade n sind. Wenn n eine Primzahl und $\alpha^n = 1$ ist, kann man für $\alpha, \beta, \gamma, \ldots$ resp. $\alpha^r, \alpha^{2r}, \alpha^{3r}, \ldots$ setzen, worin r jede beliebige der Zahlen $0, 1, 2, \ldots n-1$ vertritt. Die Demonstration stützt sich wesentlich auf die Eigenschaft der Wurzeln $\alpha, \beta, \gamma, \ldots$, dass alle ihre symmetrischen Funktionen mit Ausnahme der höchsten gleich null sind (vergl. Serret, Algèbre supérieure, 18me leçon). Man kann die ganze Auseinandersetzung beibehalten, wenn man für $\alpha, \beta, \gamma, \ldots$ Einheitswurzeln von der eben erwähnten Eigenschaft anzugeben weiss. Für komplexe Zahlen giebt es deren ausser den n komplexen Einheitswurzeln allerdings keine, für triplexe Zahlen aber kann man jede der n Horizontalgruppen der in voriger Nummer aufgestellten Tafel dafür nehmen, und hieraus geht hervor, dass die Funktion $F(x)$ auf n verschiedene Weisen in n Faktoren wie $(x-x_1)(x-x_2)\ldots(x-x_n)$ zerlegt werden kann, wodurch denn zugleich die allgemeine Form der n^2 triplexen Wurzeln der Gleichung $F(x) = 0$ nachgewiesen ist.

Auch dieses Resultat, welches dem zweidimensionalen Zahlengebiete fremd ist, legt Zeugniss für die höhere Natur der Gesetze der dreidimensionalen Zahlen ab. Zugleich gewährt dasselbe einen Einblick in die wahre Bedeutung der Beziehung, aus welcher die Meinung über die Annullirung eines Produktes ohne Annullirung einer seiner Faktoren entsprungen ist.

Die Vielheit der Wurzeln einer Gleichung n-ten Grades und die Zerlegbarkeit der Funktion $F(x)$ in n Faktoren von der Form $x-a$ beruht, wie wir schon mehrfach erwähnt haben, lediglich auf der Unbestimmtheit der Koeffizienten der Funktion F. Eine Funktion mit absolut festen Koeffizienten gestattet keine Zerlegung in binomische Faktoren oder überhaupt in Faktoren niedrigeren Grades, und eine daraus gebildete Gleichung $F(x) = 0$ wird nur durch eine einzige Wurzel identisch erfüllt. Verzichtet man aber auf die identische Erfüllung, lässt man also Werthe für x zu, welche nur dadurch die Gleichung $F(x) = 0$ erfüllen, dass man für deren Koeffizienten Werthe substituirt, die einander geometrisch decken oder gleich sind, ohne identisch zu sein; so können mehrere Werthe von x die Gleichung erfüllen und eine Zerlegung der Funktion $F(x)$ in n Faktoren ermöglichen. Ein solches Produkt deckt dann das Polynom $F(x)$ geometrisch, ist aber nicht identisch mit ihm.

Im zweidimensionalen Zahlengebiete giebt es nun lediglich eine einzige Gruppe verschiedener n Werthe von x, welche diese Bedingungen erfüllen: jeder andere zulässige Werth von x deckt einen Werth jener Gruppe, d. h. er hat die Form $xe^{2r\pi i}$ und wird demzufolge nicht für einen von x verschiedenen oder dem x ungleichen Werth gehalten. Im dreidimensionalen Gebiete dagegen giebt es n verschiedene Gruppen von je n verschiedenen Werthen von x, welche jene Bedingungen erfüllen. Die daraus gebildeten n Produkte von n Faktoren decken zwar sämmtlich das Polynom $F(x)$, d. h. ihr Endresultat oder der durch Vervielfachung und Drehung erzeugte Richtungsstrahl fällt geometrisch mit dem nach dem Endpunkte des dem Polynome $F(x)$ entsprechenden Polygons führenden Vektor zusammen: allein weder

die ersteren Produkte, noch die letzteren Polynome sind identisch dieselben. Demzufolge wird durch einen einzelnen Werth a der n^2 verschiedenen Werthe von x ein bestimmter der n^2 Faktoren $x - a$ und damit das betreffende der n Produkte, in welchem sich der Faktor $x - a$ findet, nicht aber ein anderes jener Produkte, in welchen sich $x - a$ nicht findet, annullirt. Die Annullirung eines Produktes bedingt und erfordert daher immer die Annullirung eines seiner Faktoren, aber sie verleiht möglicherweise einem anderen Produkte, welches dem ersteren zwar geometrisch gleich, aber nicht mit ihm identisch ist, einen von null verschiedenen Werth; und umgekehrt, zieht die Annullirung eines Faktors immer die Annullirung des Produktes, welchem er angehört, möglicherweise aber nicht die Annullirung eines anderen Produktes, welches dem gegebenen zwar gleich, aber nicht mit ihm identisch ist, nach sich.

Das letztere Resultat hat übrigens nur Bedeutung für das dreidimensionale, nicht für das zweidimensionale Gebiet, und kennzeichnet daher wiederholt die Gesetze des ersteren Gebietes als solche, welche in den Gesetzen des letzteren nicht enthalten sind.

Für jedes höhere Gebiet verändert sich die Vielheit der Wurzeln einer Gleichung und die Vielheit der Produkte, in welche die Funktion $F(x)$ zerlegt werden kann. Allgemein, hat die Wurzel der Gleichung n-ten Grades im m-dimensionalen Gebiete n^{m-1} verschiedene Werthe, und die Funktion $F(x)$ lässt sich auf ebenso viel verschiedene Weisen als ein Produkt von n Faktoren darstellen.

Für das dreidimensionale Gebiet ergeben sich die n^2 Wurzeln der Gleichung n-ten Grades, wenn n eine Primzahl ist und man nach Vorstehendem $\alpha = e^{\frac{2\pi}{n}i} = (-1)^{\frac{2}{n}} = (+1)^{\frac{1}{n}}$ und $\beta = e^{\frac{2\pi}{n}i_1} = (\div 1)^{\frac{2}{n}}$ $= (\div 1)^{\frac{1}{n}}$, also $\alpha^n = e^{2\pi i} = (-1)^2 = +1$ und $\beta^n = e^{2\pi i_1} = (\div 1)^2 = \div 1$, ausserdem aber γ entweder $= \alpha$, oder $= \alpha\beta$ setzt, durch den allgemeinen Ausdruck

$$x = \beta^{rs} b_0 + \beta^{rs}\gamma^r b_1 + \beta^{rs}\gamma^{2r} b_2 + \beta^{rs}\gamma^{3r} b_3 + \ldots + \beta^{rs}\gamma^{(n-1)r} b_{n-1}$$

worin für r und s irgend zwei der Zahlen 0, 1, 2, ... $(n-1)$ gesetzt werden können.

Wenn n eine zusammengesetzte Zahl ist; so ergeben sich aus dem Ausdrucke irgend einer zweidimensionalen Wurzel, welcher nach §. 15 Nr. 2

$$x = b_0 + \alpha^p b_1 + \alpha^q b_2 + \ldots$$

ist, n dreidimensionale Wurzeln für konstante Inklination, indem man diesen Ausdruck mit irgend einer Potenz von β multiplizirt, in der Form

$$x = \beta^r b_0 + \alpha^p \beta^r b_1 + \alpha^q \beta^r b_2 + \ldots$$

oder für gleichmässig variirende Deklination und Inklination, indem man in dem letzten Ausdrucke $\alpha\beta$ an die Stelle von α setzt, in der Form

$$x = \beta^r b_0 + \alpha^p \beta^{p+r} b_1 + \alpha^q \beta^{q+r} b_2 + \ldots$$

6) Die in meinen Beiträgen zur Theorie der Gleichungen §. 16 Nr. 1 angestellten Betrachtungen über Gleichheit und Identität bewegten sich auf dem Gebiete der arithmetischen Reihenbildung oder Addition oder

des geometrischen Fortschrittes: wir beabsichtigen jetzt, diese Betrachtungen für die Gebiete der übrigen Grundeigenschaften zu verallgemeinern.

Der Satz: Gleiches mit Gleichem vereinigt oder davon getrennt, Gleiches zu Gleichem addirt oder davon subtrahirt, Gleiches mit Gleichem multiplizirt oder dividirt, Gleiches auf gleiche Potenzen erhoben oder gleich hohe Wurzeln daraus gezogen, Gleiches zu gleichen Integrationsordnungen erhoben oder gleich hohe Differentiale daraus gebildet, überhaupt gleiche Operanden durch gleiche Operatoren mittelst einer Grundoperation verbunden, giebt Gleiches, ist nur für das ein- und zweidimensionale Grössengebiet evident; für das polydimensionale Gebiet ist derselbe nicht evident, in seiner Allgemeinheit sogar falsch und zu seiner Richtigstellung der Beschränkung durch eine spezielle Definition der Begriffe von Operand, Operator, Operation und Gleichheit bedürftig, welche in der gewöhnlichen vagen und unklaren Auffassung dieser Begriffe nicht liegt, und deren Nichtbeachtung zu ganz irrigen Resultaten führt. Wir stellen den Satz richtig, indem wir sagen: Grössen, welche als Resultate einer Grundoperation gleiche Operanden darstellen, mit Grössen, welche als Resultate derselben Grundoperation gleiche Operatoren darstellen, durch eben dieselbe Grundoperation miteinander verbunden, ergeben Resultate, welche im Sinne eben derselben Grundoperationen gleich sind, und fügen hinzu, dass, wenn eine dieser Bedingungen nicht erfüllt ist, sich unter Umständen ungleiche Resultate ergeben, auch dass bei vollständiger Erfüllung aller Voraussetzungen die Resultate im Sinne einer anderen, als der gedachten Grundoperation zuweilen ungleich sind.

Zur Charakterisirung des Begriffes der Gleichheit (welchen wir in §. 14 Nr. 3, §. 35 Nr. 12 und §. 36 Nr. 16 des Buches „Die Welt nach menschlicher Auffassung" behandelt und in Nr. 73 der „Grundlagen der Wissenschaft" erwähnt haben) bemerken wir, dass Identität Übereinstimmung in allen Theilen, Gliedern, Verhältnissen und sonstigen Bestandtheilen oder Eigenschaften zweier Grössen oder zweier Entstehungsprozesse, durch welche jene Grössen aus den Basen des Grössensystems erzeugt werden, bedeutet, dass aber Gleichheit nur die Übereinstimmung des Endresultates eines solchen Prozesses fordert. Für die Numeration oder den Vereinigungsprozess ist das Endresultat ein Inbegriff oder eine Menge von Bestandtheilen; zwei Grössen sind daher numerisch gleich, wenn sie hinsichtlich ihrer Quantität übereinstimmen. Für die Addition oder den Fortschritts- oder Anreihungsprozess ist das Endresultat eine Endgrenze, eine letzte Stelle oder ein erreichter Ort (Endpunkt); zwei Grössen sind daher als Fortschrittsgrössen oder Reihengrössen oder Polynome gleich, wenn sie durch sukzessiven Fortschritt in beliebigen Richtungen oder durch Anreihung oder Angliederung entstanden sind und einen gemeinsamen Anfangs- und Endpunkt haben (gleichviel, auf welchem Wege dieser Endpunkt erreicht wird). Für die Multiplikation oder den Verhältnissprozess ist das Endresultat ein Verhältniss zur Grundeinheit; zwei Grössen sind daher als Verhältnissgrössen oder Faktoren einander gleich, wenn sie durch wiederholte Verhältnissprozesse aus der Einheit entstanden sind und die hierdurch erzeugten Verhältnisse übereinstimmen, wenn also geometrisch die Grössen

durch Expansion, Drehung und Wälzung der Grundeinheit entstanden sind und in dieselbe Richtungsgrösse führen (gleichviel, durch welche Vervielfachungen, Drehungen und Wälzungen diese End-Verhältnisswerthe hervorgebracht sind). Für die Potenzirung oder den Dimensionirungs- oder Steigerungsprozess ist das Endresultat eine Dimensität oder Qualität; zwei Grössen sind daher als Potenzen oder Qualitäten einander gleich, wenn sie durch wiederholte Potenzirungsakte entstanden sind und die hierdurch erzielten Resultate durch denselben einfachen Potenzirungsakt erzeugt werden können; demnach können nur Grössen von gleichen Dimensionen, geometrisch nur Punktgrössen und Punktgrössen, nur Linien und Linien, nur Flächen und Flächen, nur Körper und Körper potenziell oder qualitativ einander gleich sein (gleichviel, durch welche Potenzirungsakte die gleichen Resultate erzielt sind). Für die Integration oder den Variations- oder Formprozess ist das Endresultat eine Zahlform, eine Funktion oder ein Bildungsgesetz, nämlich ein gesetzlicher Zusammenhang von Variabelen: zwei Grössen sind daher als Funktionen oder Formgrössen einander gleich, wenn sie durch mehrmalige Integrationsakte entstanden sind und in ihren Endergebnissen dasselbe Variabilitätsgesetz darstellen; hiernach kann geometrisch nur eine gerade Linie einer geraden Linie, nur ein Kreis einem Kreise, nur eine Parabel einer Parabel, nur ein Fünfeck einem Fünfecke, nur ein Oktaeder einem Oktaeder funktionell oder formgesetzlich gleich sein (wobei die Beschaffenheit der einzelnen Formprozesse, welche diese Gleichheit erzeugen, unwesentlich ist).

Gleichheit nach einer der eben genannten fünf Grundeigenschaften oder im Sinne eines der fünf Grundprozesse ist eine spezielle Gleichheit. Eine solche Gleichheit kann für mehrere Grundeigenschaften zugleich bestehen und wird dadurch eine allgemeinere. Wenn sie für alle Grundeigenschaften zugleich besteht, ist sie eine generelle Gleichheit. So sind z. B. zwei Grössen im Sinne aller fünf Grundprozesse zugleich einander gleich, wenn sie Monome mit gleichen Anfangs- und Endpunkten darstellen; denn alsdann erscheinen sie auch als Resultate einfacher Numerations-, Verhältniss-, Potenzirungs- und Formprozesse in der Form $e^{\alpha}\, e^{\varphi i}\, e^{\psi i_1}$.

Wenn eine Grösse das gemischte Resultat mehrerer Grundoperationen ist; so kann von einer reinen Gleichheit im Sinne des einen oder des anderen Grundprozesses überhaupt keine Rede sein, sondern nur von einer unreinen. Man kann in diesem Falle den Standpunkt in jedem einzelnen der fünf Grundprozesse nehmen und Gleichheit im Sinne dieses Prozesses für die vorherrschende erklären, welchem sich die übrigen unterordnen sollen. Thut man Diess, so erfordern die Formeln eine sachgemässe Interpretation; Manches, was vorher grundsätzlich evident war, erscheint als beweisbedürftiger Lehrsatz und mancher vorher gültige Satz verliert seine Richtigkeit. Der gewöhnliche Standpunkt, den die Mathematiker bewusst oder unbewusst einnehmen, ist der im Fortschrittsprozesse liegende, wonach die Gleichheit auf die Übereinstimmung der Endpunkte oder Grenzen bezogen wird. Solange man sich im zweidimensionalen Grössengebiete bewegt, bietet dieser Standpunkt keine Schwierigkeiten dar, weil es sich zeigt, dass auch Polynome, wenn sie als Numerationseinheiten, Faktoren, Exponenten und Integrationsgrade

genommen werden, in der Entwicklung des Resultates zu einem resultirenden Polynome die Gleichheit im Sinne des Fortschrittsgesetzes gewährleisten. Diese Wahrheit ist keine grundsätzliche, sondern eine durch Beweise sich ergebende. Es kann gezeigt werden, dass, wenn $a, b, c, \ldots$ beliebige reelle oder komplexe Grössen bedeuten und die Gleichheit im Sinne des Fortschrittsgesetzes genommen wird, nicht allein $a + b = b + a$, $a\,b = b\,a$, sondern auch $(a + b)\,(c + d) = a\,c + a\,d + b\,c + b\,d$, $a^{b+c} = a^b\,a^c$ u. s. w. ist, dass also, wenn $a = b + c$ und $d = e + f$ ist, $a + d = b + c + e + f$, $a\,d = (b + c)\,(e + f) = b\,e + b\,f + c\,e + c\,f$, $a^d = (b + c)^{e+f} = (b + c)^e\,(b + c)^f$ und wenn unter d eine Funktion $F(x) = f(x) + g(x)$ verstanden wird, $\int F(x)\,\partial x = \int [f(x) + g(x)]\,\partial x = \int f(x)\,\partial x + \int g(x)\,\partial x$ ist. Ebenso ist, wenn man $a = b\,c$, $d = e\,f$ und $F(x) = f(x)\,g(x)$ hat, auch $a + d = b\,c + e\,f$, $a\,d = b\,c\,e\,f$, $a^d = (b\,c)^{e\,f} = b^{e\,f}\,c^{e\,f}$ und $\int F(x)\,\partial x = \int f(x)\,g(x)\,\partial x$. Ferner ist, wenn man $a = b^c$, $d = e^f$ und $F(x) = f(x)^{g(x)}$ hat, $a + d = b^c + e^f$, $a\,d = b^c\,e^f$, $a^d = (b^c)^{e^f} = b^{c\,e^f}$ und $\int F(x)\,\partial x = \int f(x)^{g(x)}\,\partial x$. Endlich ist, wenn man $a = f_1(b)$, $d = f_2(e)$ und $F(x) = f[g(x)]$ hat, $a + d = f_1(b) + f_2(e)$, $a\,d = f_1(b)\,f_2(e)$, $a^d = f_1(b)^{f_1(e)}$, $\int F(x)\,\partial x = \int f[g(x)]\,\partial x$.

Diese Sätze haben aber nur für das zweidimensionale Gebiet Gültigkeit, für das drei- und mehrdimensionale Gebiet sind sie fast alle falsch. Wehn $a, b, c, \ldots$ dreidimensionale Grössen sind, behalten nur die Sätze, dass, wenn $a = b + c$ und $d = e + f$ ist, auch $a + d = b + c + e + f$ sei, sowie der Satz, dass, wenn $a = b\,c$ und $d = e\,f$ ist, auch $a\,d = b\,c\,e\,f$ sei, Gültigkeit: alle übrigen aber werden unrichtig, insbesondere bedingt die Gleichheit $a = b + c$, $d = d$ nicht die Gleichheit $a\,d = b\,d + c\,d$ oder, die Gleichung $(b + c)\,d = b\,d + c\,d$ ist im Allgemeinen unrichtig, es darf also, ohne die Gleichheit zu verletzen, das Produkt von Polynomen wie $(a + b)\,(c + d)$ nicht nach den gewöhnlichen Formeln in Partialprodukte entwickelt werden. Wenn

$$e^{\alpha i}\,e^{\alpha_1 i_1} = e^{\beta i}\,e^{\beta_1 i_1} + e^{\gamma i}\,e^{\gamma_1 i_1}$$

ist; so hat die Grösse $e^{\alpha i}\,e^{\alpha_1 i_1}\,.\,e^{\delta i}\,e^{\delta_1 i_1}$, welche gleich $e^{(\alpha+\delta)i}\,e^{(\alpha_1+\delta_1)i_1}$ ist, einen ganz anderen Endpunkt, als die Grösse $(e^{\beta i}\,e^{\beta_1 i_1} + e^{\gamma i}\,e^{\gamma_1 i_1})\,e^{\delta i}\,e^{\delta_1 i_1}$, welche gleich $e^{(\beta+\delta)i}\,e^{(\beta_1+\delta_1)i_1} + e^{(\gamma+\delta)i}\,e^{(\gamma_1+\delta_1)i_1}$ ist, beide decken sich durchaus nicht, wennicht zufällig $\beta_1 = \gamma_1$ oder $\beta_1 = \gamma_1 + n\,\pi$ (worin n eine ganze Zahl) ist, oder wennicht $\delta = 0$ oder $\delta = n\,\pi$ ist. Wir stossen also bei diesem Resultate auf eine neue wesentliche Verschiedenheit der Gesetze des zwei- und dreidimensionalen Gebietes.

Nach Vorstehendem ist auch, wenn $b + c + d = 0$ ist, keineswegs allgemein $a\,b + a\,c + a\,d = 0$; insbesondere hat, wenn $e^{\alpha i}e^{\alpha_1 i_1} + e^{\beta i}\,e^{\beta_1 i_1} + e^{\gamma i}\,e^{\gamma_1 i_1} = 0$ ist, die durch partielle Multiplikation mit $e^{\delta i}\,e^{\delta_1 i_1}$ entstehende Summe von Produkten $e^{(\alpha+\delta)i}\,e^{(\alpha_1+\delta_1)i_1} + e^{(\beta+\delta)i}\,e^{(\beta_1+\delta_1)i_1} + e^{(\gamma+\delta)i}\,e^{(\gamma_1+\delta_1)i_1}$ im Allgemeinen einen von null verschiedenen Werth, wenn also auch das Polynom $b + c + d$ geometrisch ein geschlossenes Raumpolygon darstellt; so stellt doch nicht in allen Fällen das Polynom $a\,b + a\,c + a\,d$ ebenfalls ein geschlossenes Polygon dar.

Wäre $b + c = 0$; so würde auch $ab + ac = 0$ sein, weil in diesem speziellen Falle, wo $b = -c$ ist, die Bedingung $\beta_1 = \gamma_1 + n\pi$ erfüllt ist.

Das Vorstehende lehrt auch, dass, wenn $a + b = 0$ und $c + d = 0$ ist, nicht unbedingt $ac + ad + bc + bd = 0$ sein wird, und hieraus folgt, dass, wenn die n annullirten Binome $x - x_1 = 0$, $x - x_2 = 0, \ldots$ $x - x_n = 0$ miteinander multiplizirt und nach gewöhnlichen Multiplikationsregeln in ein Polynom entwickelt werden, keineswegs dieses Polynom $x^n - (x_1 + x_2 + \ldots)x^{n-1} + (x_1x_2 + x_2x_3 + \ldots)x^{n-2} - \ldots = 0$ sein wird, während doch das unentwickelte Produkt $(x-x_1)(x-x_2)\ldots(x-x_n)$, wenn man jeden Faktor als einfache Verhältnissgrösse in der Form $ae^{\alpha i}\, e^{\alpha_1 i_1}$, $be^{\beta i}\, e^{\beta_1 i_1}$, $ce^{\gamma i}\, e^{\gamma_1 i_1}$ u. s. w. darstellt, sicher $= 0$ ist.

Auf den ersten Blick könnte dieser Satz Zweifel an der Richtigkeit unserer Deduktion in Nr. 4 und 5 erwecken: jedoch mit Unrecht. Wir haben dort kein Produkt aus annullirten Binomen gebildet (die Binome $x - x_1$, $x - x_2$ u. s. w. können überhaupt nicht alle auf einmal oder für denselben Werth von x gleich null sein); vielmehr haben wir das Produkt $(x - x_1)(x - x_2)\ldots$ durch Ausführung der partiellen Multiplikationen in ein Polynom $x^n - (x_1 + x_2 + \ldots)x^{n-1} +$ u. s. w. verwandelt, dieses Polynom mit dem Polynome gleichen Grades $x^n + a_1x^{n-1} + \ldots$ durch Gleichsetzung der Koeffizienten gleich hoher Glieder identifizirt und gesagt, dass, wenn letzteres Polynom für gewisse Werthe von x gleich null sei, auch ersteres für dieselben Werthe gleich null sein müsse, was ein einwandsfreier Schluss ist. Ausserdem haben wir behauptet, dass, wenn in dem unentwickelten Produkte $(x - x_1)(x - x_2)\ldots$ ein Faktor gleich null sei, auch das Produkt den Nullwerth habe und dass dieses Produkt (welches, wenn es nicht in Glieder zerlegt ist, kein Polynom, sondern eine Verhältnissgrösse darstellt) nur dann gleich null sein könne, wenn einer seiner Faktoren gleich null ist, was ebenfalls volle Wahrheit enthält. Wir bemerken noch, dass das erste Resultat vornehmlich eine Gleichheit im Sinne des Fortschrittsgesetzes, das zweite dagegen eine Gleichheit im Sinne des Verhältnissgesetzes vor Augen hat.

Die letzteren Erläuterungen haben wir auf die Gleichheit im Sinne des Fortschritts-, des Verhältniss-, des Steigerungs- und des Formprozesses bezogen, ohne die Gleichheit im Sinne des Vereinigungsprozesses, welcher der ursprünglichste von allen ist, zu berücksichtigen. Wir fügen daher hinzu, dass für diese Gleichheit immer die Formeln $a + b = b + a$, $(a + b)(c + d) = ac + ad + bc + bd$, $a^{b+c} = a^b a^c$, worin das Zeichen $+$ soviel wie „eingeschlossen" oder „und" und das Zeichen $-$ soviel wie „ausgeschlossen" bedeutet, Gültigkeit haben, dass jedoch eine Zerlegung der einfachen Verhältnissgrösse $e^{\alpha i}$ in zwei Bestandtheile $\cos\alpha$ und $\sin\alpha \,.\, i$ oder eine Vereinigung zweier solchen Bestandtheile zu dem Werthe $e^{\alpha i}$ unzulässig ist, weil $e^{\alpha i}$ durchaus nicht ein Inbegriff eines reellen und eines imaginären Bestandtheiles, sondern eine durch Fortschritt vom Endpunkte des reellen Gliedes in der Seitenrichtung um den Betrag des imaginären Gliedes entstehende Summe oder ein zusammenhängendes, vergliedertes Polynom ist. Bei Zugrundelegung der Gleichheit im Sinne des Vereinigungsprozesses kann man daher, selbst wenn $a, b, c, \ldots$ polydimensionale Werthe haben, die Formeln der

niederen Mathematik, jedoch nicht die für imaginäre und komplexe Grössen gültigen Formeln der höheren Algebra, also unter Anderem nicht die Formel $e^{ai} = a + bi$ und noch weniger die Formel $e^{ai}\, e^{\beta i_1} = a + bi + cii_1$ in Anwendung bringen. Unbedenklich kann man also in diesem Sinne $(a + bi)\ (c + di) = ac + (ad + bc)i + bdi^2$, ferner $(a + bi + cii_1)\ (a' + b'i + c'ii_1) = aa' + (ab' + a'b)i + bb'i^2 + (ac' + a'c)ii_1 + (bc' + b'c)i^2 i_1 + cc'i^2 i_1^2$ setzen, darf jedoch Zusammenziehungen und Zerlegungen nach den zuvor genannten Formeln nicht vornehmen, wenn man nicht Gefahr laufen will, die gröbsten Irrthümer zu begehen (vergl. weiter unten den §. 18 über die Quaternion).

Unzweifelhaft kann man jeden auf irgend einer festen Regel beruhenden Vorgang benutzen, um damit Gebilde herzustellen und gesetzlich zu verändern, auch die entsprechenden Resultate und Operationen sinnbildlich in Formeln kleiden. Man könnte also beschliessen, gewisse Formeln der niederen und der höheren Mathematik ohne Rücksicht auf den oben erörterten logischen Begriff der Gleichheit in Anwendung zu bringen, also z. B. ohne Weiteres für alle Grössengebiete das Produkt von Polynomen in eine Summe von Partialprodukten auflösen oder für $(a + b)\ (c + d)$ den Ausdruck $ac + dd + bc + bd$ substituiren. Diess mag jedem Mathematiker unverwehrt sein: allein, es ist ihm verwehrt, den Ergebnissen solcher Rechnungen eine Bedeutung beizulegen, welche nur für diejenigen Gebiete eine nachweisbare Gültigkeit hat, welchen jene Formeln entnommen sind. Das, was bei einer solchen willkürlichen Anwendung von Formeln gleich genannt wird, entspricht dann nicht mehr den gewöhnlichen Vorstellungen von Gleichheit, sondern nur einer gewissen rechnungsmässigen Beziehung, welche sich von der Vorstellung einer Übereinstimmung in Endpunkten oder Endresultaten sehr weit entfernen kann; namentlich verschwindet bei einer solchen Rechnungsweise die Analogie zu den korrespondirenden Raumgestalten, und die Gleichheit der Rechnungsresultate hat nicht mehr die Bedeutung der geometrischen Deckung. Bei einer solchen Rechnungsweise erscheint es daher unangemessen, sich des Zeichens $=$ zu bedienen, um damit eine Eigenschaft zu bezeichnen, welche einer Übereinstimmung entspricht. Gleichwie Gauss für die aus gewissen Operationen hervorgehenden Resultate, die eine bestimmte Beziehung zu einander haben, ohne eigentlich gleich zu sein, die also nur in gewisser, auf einer Rechnungsoperation beruhenden Beziehung äquivalent sind, das Zeichen eingeführt hat; so müsste auch für die Resultate der erwähnten Rechnung statt des Zeichens $=$ und des Ausdruckes gleich ein anderes Zeichen und ein anderer Ausdruck gebraucht werden.

Auf den Titel eines rationellen Verfahrens könnte aber eine Operation mit Ungleichheitszeichen und Ungleichheitsbegriffen, welche die Analogie zwischen der abstrakten Formel und der geometrischen Anschauung vernichtet, keinen Anspruch erheben, und selbst die Berufung auf das Gausssche Kongruenzzeichen $\equiv$ wäre unberechtigt, da dieses Zeichen doch immer eine Übereinstimmung in einer bestimmten Eigenschaft (nämlich in dem Reste) als wesentliche Bedingung fordert. Die Unangemessenheit eines solchen Verfahrens würde sich aber wegen seiner gänzlichen Entbehrlichkeit wesentlich steigern. Der Begriff der Übereinstimmung in gewissen Eigenschaften oder Beziehungen ist die naturgemässe und darum

beste, ja für die allgemeine Mathematik die einzige brauchbare Grundlage der Vergleichung der Grössen untereinander. Um diese Übereinstimmung zu sichern, brauchen für die höheren Gebiete nur wenige geeignete Maassregeln beobachtet zu werden. Für die aus Additionen und Multiplikationen sich zusammensetzenden Operationen mit unseren polydimensionalen Grössen reichen folgende Regeln aus.

Eine Verhältnissgrösse $r e^{\varphi i} e^{\psi i_1}$ ist stets dem Trinome $r \cos\varphi + r \sin\varphi \cos\psi \,.\, i + r \sin\varphi \,.\, \sin\psi \,.\, i i_1$ welches anzeigt, dass der Endpunkt der mit Deklinations- und Inklinations-Koeffizienten behafteten Grösse von der Quantität r durch einen gegliederten Koordinatenzug erreicht wird, stets gleich zu setzen, oder der eine Werth kann für den anderen substituirt werden, wenn mit dieser Substitution die Operation schliesst. Soll jedoch die Operation weitergeführt werden; so ist die Substitution nur zulässig, so lange es sich um Additionen handelt, d. h. man kann immer

$$r e^{\alpha i} e^{\alpha_1 i_1} + s e^{\beta i} e^{\beta_1 i_1} = (a_1 + a_2 i + a_3 i i_1) + (b_1 + b_2 i + b_3 i i_1)$$
$$= (a_1 + b_1) + (a_2 + b_2) i + (a_3 + b_3) i i_1$$

setzen. Die Substitution ist dagegen unzulässig, wenn es sich um Multiplikationen handelt; zu solchem Zwecke müssen beide Faktoren zuvor in die Form $r e^{\alpha i} e^{\alpha_1 i_1}$ von Verhältnissgrössen gebracht, es muss also ein Faktor, wenn er als Trinom $a_1 + a_2 i + a_3 i i_1$ gegeben ist, vorher in die Form $r e^{\alpha i} e^{\alpha_1 i_1}$ gebracht werden, indem man

$$r = \sqrt{a_1^2 + a_2^2 + a_3^2}$$

$$\cos\alpha = \frac{a_1}{\sqrt{a_1^2 + a_2^2 + a_3^2}} \qquad \sin\alpha = \sqrt{\frac{a_2^2 + a_3^2}{a_1^2 + a_2^2 + a_3^2}}$$

$$\cos\beta = \frac{a_2}{\sqrt{a_2^2 + a_3^2}} \qquad \sin\beta = \frac{a_3}{\sqrt{a_2^2 + a_3^2}}$$

setzt und das Produkt nach der immer gültigen Formel

$$r e^{\alpha i} e^{\alpha_1 i_1} \times s e^{\beta i} e^{\beta_1 i_1} = r s e^{(\alpha+\beta) i} e^{(\alpha_1+\beta_1) i_1}$$

vollzieht. Wegen der Verschiedenheit der Bedeutung haben wir die Verhältnissgrösse $e^{\varphi i} e^{\psi i_1}$ den vollständigen, das Polynom $\cos\varphi + \sin\varphi \cos\psi \,.\, i + \sin\varphi \sin\psi \,.\, i i_1$ dagegen den abgekürzten Richtungskoeffizienten genannt.

7) Wenn man mit diesen Auffassungen Untersuchungen über die Zerlegung der Zahlen in ganze Faktoren anstellen will, muss zuvor der Begriff einer ganzen Zahl festgestellt werden. Für das ein- und zweidimensionale Gebiet steht derselbe fest, indem $a + b i$ für eine ganze Zahl gilt, wenn a und b ganze reelle Werthe haben. Behält man den hierin liegenden Grundgedanken bei; so ist die drei- und mehrdimensionale Zahl eine ganze, wenn sie ganze Koordinaten hat, worin unter Koordinaten die gegeneinander neutralen Glieder a, $b i$, $c i i_1$ u. s. w. des Polynoms $a + b i + c i i_1 +$ u. s. w., entsprechend den geometrischen rechtwinkligen Koordinaten, verstanden sind. Dass das Produkt zweier ganzen Zahlen, wenn eine oder beide einem höheren, als dem zweidimensionalen Gebiete angehören, nicht nothwendig eine ganze Zahl,

sondern meistens eine gebrochene oder irrationale Zahl ist, und dass ferner das Produkt einer ganzen mit einer unganzen Zahl ein ganzes Produkt geben kann, leuchtet ein und charakterisirt aufs Neue die Gesetze der höheren Zahlengebiete als eigenartige.

Bei dieser natürlichen Auffassung habe ich in der Schrift über die „polydimensionalen Grössen“ §. 8 gezeigt, dass der Begriff einer Primzahl unbestimmt ist, solange das Zahlengebiet, aus welchem die Faktoren genommen werden sollen, nicht bestimmt ist. Demzufolge nennen wir eine gemeine n-dimensionale Primzahl diejenige, welche sich in keine n-dimensionalen oder niedriger dimensionirten Faktoren zerlegen lässt, ferner eine n-dimensionale Zahl eine relative Primzahl vom r-dimensionalen Faktorengebiete eine solche, welche sich in keine r-dimensionalen oder niedriger dimensionirten Faktoren zerlegen lässt, endlich eine absolute oder vollkommene Primzahl eine solche, welche sich in keine Faktoren irgend eines Gebietes zerlegen lässt.

Bekannt ist bereits, dass eine reelle Primzahl wie 5, 17, 29 u. s. w., welche sich als die Summe zweier Quadrate $a^2 + a_1{}^2$ darstellen lässt, keine absolute Primzahl ist, indem sie sich in die beiden komplexen Faktoren $a + a_1 i$ und $a - a_1 i$ zerlegen lässt. Wir haben diesem Satze die folgenden hinzugefügt.

Jede reelle Primzahl, welche sich als die Summe dreier Quadrate darstellen lässt, wie 3, 11, 19, 29 u. s. w., ist keine absolute Primzahl, sondern lässt sich in zwei triplexe Faktoren zerlegen. Eine solche Zerlegung kann aber auf mehrfache Weise geschehen; so hat man z. B. für $29 = 4^2 + 3^2 + 2^2$ die Zerlegung $(4 + 3i + 2ii_1)(4 - 3i + 2ii_1)$, aber auch $(3 + 4i + 2ii_1)(3 - 4i + 2ii_1)$, ferner $(2 + 3i - 4ii_1)(2 - 3i - 4ii_1)$ u. s. w. Für 17 hat man zwei verschiedene Zerlegungen $1^2 + 4^2$ und $2^2 + 2^2 + 3^2$, es ist daher sowohl $1 + 4i$, als auch $2 + 2i + 3ii_1$ ein Faktor von 17.

Jede reelle Primzahl, welche sich als eine Summe von n Quadraten darstellen lässt, ist keine vollkommene Primzahl, sondern ein Produkt von zwei n-dimensionalen Faktoren und zwar in mehrfacher Weise.

Da sich jede reelle Zahl als Summe von 4 und mehr Quadraten darstellen lässt; so ist keine reelle Primzahl eine absolute, sondern immer in zwei ganze Faktoren irgend welcher Gebiete in mehrfacher Weise zerlegbar.

Was die gemeinen Primzahlen der höheren Gebiete betrifft; so ist jede gemeine komplexe Primzahl eine vollkommene, d. h. sie ist in keine ganzen Faktoren irgend eines Gebietes zerlegbar. Das Nämliche gilt von den gemeinen triplexen Primzahlen. Übrigens können manche zwei triplexe Primzahlen dasselbe Produkt hervorbringen, wie zwei andere triplexe oder duplexe Primzahlen. Manche Zahl lässt sich daher in verschiedener Weise in absolute Primfaktoren zerlegen.

Überhaupt ist diejenige Zahl $a + bi + cii_1 + \ldots$ eine vollkommene Primzahl, deren Norm $a^2 + b^2 + c^2 + \ldots$ eine gemeine reelle Primzahl ist. Hierdurch sind die reellen Zahlen, mit Ausnahme der 1, sämmtlich von den vollkommenen Primzahlen ausgeschlossen, und es giebt unter den reellen Primzahlen sowohl ge-

meine (welche keine reellen Faktoren haben), als auch relative (welche sich in höher dimensionirte Faktoren zerlegen lassen). Ferner leuchtet ein, dass es unter den höher dimensionirten Zahlen nur vollkommene Primzahlen giebt, indem alle gemeinen Primzahlen dieser Gebiete zugleich absolute sind (welche sich weder in gleichdimensionirte, noch in höher oder niedriger dimensionirte Faktoren zerlegen lassen).

Dem Vorstehenden zufolge giebt es in jedem Grössengebiete, nur nicht im reellen, unzerlegbare ganze Zahlen oder Primzahlen, welche Primfaktoren für die zerlegbaren Zahlen sind. Die zerlegbaren Zahlen des drei- und mehrdimensionalen Gebietes scheinen eine mehrfache Zerlegung in verschiedene Primfaktoren zu gestatten und sich dadurch von den ganzen reellen und komplexen Zahlen zu unterscheiden: allein, dieser Unterschied ist nur ein scheinbarer, welcher bei genauerer Erwägung vollständig verschwindet. Die Zerlegbarkeit der reellen und die der komplexen Zahlen in Primfaktoren ist durchaus keine einzige, sondern stets eine mehrfache, selbst wenn man den Unterschied in der Reihenfolge der Faktoren ganz ausser Acht lässt, also diese Faktoren nach ihrer Grösse und ihrer Richtungsabweichung von der Einheit ordnet. Denn man hat im reellen Gebiete nicht nur $5 = 1 \,.\, 5$, sondern auch $= (-1) \,.\, (-5)$ und im komplexen Gebiete nicht nur die eben genannten beiden Zerlegungen von 5, sondern auch die Zerlegungen $(i)\,(-5i)$, $(-i)\,(5i)$, $(1+2i)\,(1-2i)$, $(2+i)\,(2-i)$, $(-1+2i)\,(-1-2i)$ und mehrere andere. Im reellen Gebiete gilt 5 als Primzahl, lässt aber dennoch die beiden verschiedenen Zerlegungen $1 \,.\, 5$ und $(-1) \,.\, (-5)$ zu: man beseitigt diese Verschiedenheit, indem man sagt, die reelle Primzahl p habe ausser der Einheit 1 und ihrem eigenen Werthe p keine anderen Faktoren, als solche, welche sich von diesen beiden nur durch ein Zeichen oder durch einen Richtungskoeffizienten unterscheiden: denn -1 und -5 unterscheiden sich bezw. von 1 und 5 nur durch den Richtungskoeffizienten -1.

Der nämliche Satz gilt dann auch für das komplexe Gebiet. Hier ist 5 nicht mehr eine Primzahl, also auch $5i$ nicht. Wohl aber sind hier $1+2i$, $1-2i$, $2+i$, $2-i$, $-1-2i$, $-1+2i$, $-2+i$, $-2-i$ Primzahlen: dieselben unterscheiden sich jedoch nur durch den Richtungskoeffizienten -1 oder i oder $-i$.

Wir stellen nun den allgemeinen, für alle Zahlengebiete gültigen Satz auf. Zwei polyplexe Zahlen $a + a_1 i + a_2 i i_1 + \ldots$ und $b + b_1 i + b_2 i i_1 + \ldots$ von gleicher Norm, für welche also $a^2 + a_1^2 + a_2^2 + \ldots = b^2 + b_1^2 + b_2^2 + \ldots$ ist (mag die Norm eine ganze oder eine unganze reelle Zahl sein), unterscheiden sich von einander nur durch einen Faktor, welcher ein Richtungskoeffizient ist, welcher also eine in einer bestimmten Richtung gemessene Einheit darstellt: wir nennen solche Zahlen äquivalente Faktoren. Dieser Satz, welcher für triplexe Zahlen sagt, dass, wenn $c = r e^{\varphi i} e^{\psi i_1}$ und $c_1 = r e^{\varphi_1 i} e^{\psi_1 i_1}$ ist, also c und c_1 dieselbe Norm r^2 haben, $c = c_1 e^{(\varphi-\varphi_1) i} e^{(\psi-\psi_1) i_1}$ sein wird, ergiebt sich aus unserer Theorie der polydimensionalen Zahlen auf den ersten Blick.

Hiernach unterscheidet sich irgend eine der komplexen Zahlen $a+bi$, $a-bi$, $b+ai$, $b-ai$, $-a-bi$, $-a+bi$, $-b-ai$, $-b+ai$

von der anderen nur durch einen Richtungskoeffizienten $e^{\varphi i}$. Es unterscheiden sich aber auch die triplexen und komplexen Zahlen $2+3i+4ii_1$, $3+4i+2ii_1$, $4-2i+3ii_1$, $2+5i$, $5-2i$ u. s. w., da sie sämmtlich die Norm 29 haben, nur durch einen Richtungskoeffizienten $e^{\varphi i}\, e^{\psi i_1}$; sie sind also äquivalente Faktoren.

Wenn die Norm eine ganze reelle Zahl ist, kann es offenbar nur eine endliche Menge ganzer äquivalenter Zahlen von einer bestimmten höchsten Dimensität, und wenn man die Dimensität unbeschränkt lässt, doch immer nur eine endliche Anzahl verschiedener Werthe von $a, a_1, a_2, \ldots$ geben. Diese Zahlen kann man so ordnen, dass, wenn sie durch $re^{\varphi i}\, e^{\psi i_1}$, $re^{\varphi_1 i}\, e^{\psi_1 i_1}$, $re^{\varphi_2 i}\, e^{\psi_2 i_1}$ u. s. w. dargestellt sind, φ den kleinsten Deklinations-, ψ den kleinsten Inklinationswinkel u. s. w. bezeichnet (was nicht ausschliesst, dass mehrere aufeinander folgende Deklinationswinkel φ_1, φ_2 dem φ gleich seien). Die erste dieser Zahlen kann als die niedrigste aller äquivalenten Zahlen angesehen werden, da sie die kleinste Abweichung von der Einheit 1 zeigt: man kann sie zum Vertreter aller äquivalenten Zahlen annehmen. Da der kleinste Werth von φ dem grössten Werthe von $\cos\varphi$ entspricht, in der triplexen Zahl $A = a + a_1 i + a_2 ii_1$ aber $\cos\varphi = \dfrac{a}{\sqrt{a^2 + a_1^2 + a_2^2}}$ ist; so entspricht, weil die Norm aller in Betracht kommenden Zahlen gleich $a^2 + a_1^2 + a_2^2$ ist, der kleinste Werth von φ dem grössten Werthe des positiv genommenen reellen Gliedes a. In Erwägung, dass $\sin\varphi\cos\psi = \dfrac{a_1}{\sqrt{a^2 + a_1^2 + a_2^2}}$, mithin $\cos\psi = \dfrac{a_1}{\sqrt{a_1^2 + a_2^2}} = \dfrac{1}{\sqrt{1 + \left(\frac{a_2}{a_1}\right)^2}}$ ist; so entspricht der kleinste Werth von ψ oder der grösste Werth von $\cos\psi$ dem kleinsten Werthe des Verhältnisses $\dfrac{a_2}{a_1}$ oder dem grössten Werthe des Verhältnisses $\dfrac{a_1}{a_2}$, während a_1 und a_2 positiv zu nehmen sind. Hiernach ist z. B. von allen ganzen Zahlen, welche die Norm 29 haben, die komplexe Zahl $5 + 2i$ die niedrigste. Dieselbe ist niedriger, als jede der ihr äquivalenten triplexen Zahlen, während unter diesen selbst die Zahl $4 + 3i + 2ii_1$ die relativ niedrigste ist.

Indem die Norm einer Zahl eine Zerlegung in Quadrate wie $a^2 + a_1^2 + a_2^2 + \ldots$ zulässt, gestattet sie immer mehrere solche Zerlegungen, da jede Verstellung der Quadrate der ersten Zerlegung als eine andere Zerlegung aufgefasst werden kann, ausserdem aber für jedes einzelne a sein negativer Werth $-a$ gesetzt werden kann. Hieraus folgt: Wenn sich eine Zahl in mehrfacher Weise in verschiedene Faktoren zerlegen lässt, welche dieselbe Norm beibehalten, wenn also in der Zerlegung $c = p\, p_1\, p_2 = q\, q_1\, q_2$ die ersten beiden Faktoren p und q, sowie auch die zweiten beiden Faktoren p_1 und q_1, ferner die dritten beiden Faktoren p_2 und q_2 gleiche Norm haben; so

können sich die ersten, zweiten, dritten beiden Faktoren nur durch einen Richtungskoeffizienten unterscheiden, oder sie sind äquivalent: wenn also ϱ, ϱ_1, ϱ_2, ... verschiedene Richtungskoeffizienten sind; so ist $q = \varrho p$, $q_1 = \varrho_1 p_1$, $q_2 = \varrho_2 p_2$ u. s. w.

Ausserdem liegt es auf der Hand, dass, wenn die Richtungskoeffizienten ϱ, ϱ_1, ϱ_2, ... zusammengefasst werden, ihr Produkt $\varrho\, \varrho_1\, \varrho_2 = 1$ sein muss.

Da jede zusammengesetzte reelle Zahl in reelle Primfaktoren zerfällt; so können die echten Primfaktoren (mag man darunter gemeine, relative oder absolute verstehen) nur unter den Faktoren der reellen Primzahlen gesucht werden. Nun ergiebt sich aus unserer Theorie ferner der Satz: Im allgemeinen polydimensionalen Zahlengebiete ist jede reelle Primzahl p das Produkt zweier ganzen Faktoren p_1, p_2 von gleicher Norm p, welche sich nur durch ihre Richtungskoeffizienten ϱ_1, ϱ_2 in der Art unterscheiden, dass $\varrho_1\, \varrho_2 = 1$ ist. Diese Faktoren sind absolute Primfaktoren, aber einander äquivalent. Gestattet die Zahl p verschiedene Zerfällungen in Quadrate; so liefert Diess doch immer nur Primfaktoren p_1, p_2 von der Norm p, welche sich lediglich durch Richtungskoeffizienten von den übrigen Primfaktoren der Zahl p unterscheiden, also einander und jedem anderen Primfaktor von p äquivalent sind. Betrachtet man nicht absolute, sondern gemeine Primzahlen von gegebener Dimensität n; so ist es möglich, dass sich die reelle Primzahl p nicht in n oder weniger als n Quadrate zerfällen lässt: alsdann ist p selbst ein Primfaktor für das n-dimensionale Gebiet.

Ist $A = a + a_1 i + a_2 i i_1 + \ldots$ irgend eine reelle, komplexe oder polyplexe Zahl; so ist ihre Norm $a^2 + {a_1}^2 + {a_2}^2 + \ldots$ das Produkt von Potenzen einer gewissen Anzahl n von reellen Primzahlen p_1, p_2, ... p_n, also $N(A) = p_1^{a_1}\, p_2^{a_2} \ldots p_n^{a_n}$. Bezeichnen nun P_1, P_2, ... P_n ebenfalls n absolute Primzahlen resp. von den Normen p_1, p_2, ... p_n; so ist immer $A = P_1^{a_1}\, P_2^{a_2} \ldots P_n^{a_n}$, in welchem Produkte P_1, P_2, ... P_n jeden äquivalenten Primfaktor bezw. von der Norm p_1, p_2, ... p_n vertritt. Jede ganze Zahl A ist daher aus absoluten Primfaktoren ebenso zusammengesetzt, wie ihre reelle Norm aus gemeinen reellen Primzahlen zusammengesetzt ist. Diese Zusammensetzung ist eine einzige, wenn man unter P_1, P_2, ... P_n die Vertreter äquivalenter Primfaktoren versteht, sodass sie auch durch die je niedrigsten Primfaktoren der betreffenden Normen ersetzt werden können.

Wenn man will, kann man für die Potenz eines Primfaktors, also für $P_1^{a_1}$ das Produkt von a_1 äquivalenten Primfaktoren P_1', P_1'', P_1''', ... setzen, sodass $P_1^{a_1} = P_1'\, P_1''\, P_1''' \ldots$ ist. Auf diese Weise und durch Zusammenfassung von beliebig vielen solchen Faktoren erscheint die Zahl A auf verschiedene Weise in Faktoren zerlegt, die jedoch nur Produkte der n absoluten Primfaktoren P_1, P_2, ... P_n oder ihrer äquivalenten Werthe sind.

Für eine reelle Primzahl $A = p$ ist die Norm $= p^2$; sie ist also keine absolute Primzahl, sondern das Quadrat einer solchen, nämlich $= P_1^2$, oder das Produkt aus zwei mit P_1 äquivalenten Primzahlen $P_1' P_1''$. So ist z. B. $5 = [(1 + 2i) e^{\varphi i}]^2$ und auch $= (1 + 2i) \cdot (1 + 2i) e^{2\varphi i}$, auch $= (1 + 2i)(1 - 2i)$, indem $1 - 2i = (1 + 2i) e^{2\varphi i}$ ist, woraus sich für $e^{2\varphi i} = \cos 2\varphi + \sin 2\varphi \cdot i$ der Werth $-\frac{3}{5} - \frac{4}{5} i$ ergiebt, der einem Richtungskoeffizienten entspricht, da seine Norm $= 1$ ist.

Ist die Norm der Zahl A eine reelle Primzahl p, z. B. $= 29$; so ist $A = P_1$ immer eine absolute Primzahl, welche nur durch eine äquivalente ersetzt werden kann.

Die Norm der Zahl $A = 2 + 4i + 5 i i_1$ ist $45 = 3^2 5$. Demzufolge ist $A = P_1^2 P_2$. Da $3 = 1^2 + 1^2 + 1^2$ und $5 = 1^2 + 2^2$ ist; so ist der niedrigste der äquivalenten Primfaktoren P_1 gleich $1 + i + i i_1$ und der niedrigste der äquivalenten Primfaktoren P_2 gleich $2 + i$. Hiernach hat man

$$2 + 4i + 5 i i_1 = [(1 + i + i i_1) e^{\varphi i} e^{\psi i_1}]^2 [(2 + i) e^{\varphi_1 i} e^{\psi_1 i_1}]$$

Aus allem Diesen geht hervor, dass alle gemeinen Primzahlen eines bestimmten Gebietes und alle absoluten Primzahlen des Gesammtgebietes und deren äquivalente Werthe durch Zerfällung der reellen Primzahlen in Quadrate gefunden werden und dass sich aus diesen Primzahlen jede Zahl jedes Gebietes auf einzige Weise, d. h. aus Primfaktoren von ganz bestimmter Anzahl und ganz bestimmten Normen, welche sich bei verschiedenen Zerlegungen lediglich durch Richtungskoeffizienten unterscheiden, zusammensetzt.

Hierdurch verschwindet jede Verschiedenheit zwischen den Gesetzen der Theilbarkeit reeller, komplexer und überkomplexer Zahlen von beliebiger Dimensität.

Wir bemerken noch, dass offenbar kein Faktor einer polydimensionalen Zahl, mag er ein Primfaktor sein, oder nicht, null werden kann, ohne dass das Produkt null wird, und, umgekehrt, bedingt die Annullirung eines Produktes die Annullirung eines seiner Faktoren, wobei es irrelevant ist, ob man die Zahlen in der Form $r e^{\varphi i} e^{\psi i_1}$ oder als Polynome in der Form $a + a_1 i + a_2 i i_1 + \ldots$ darstellt: denn die Annullirung einer Zahl in der ersten Form verlangt $r = 0$ und in der zweiten Form zugleich $a = 0$, $a_1 = 0$, $a_2 = 0$ u. s. w.

§. 18. Die ideale Zahl.

1) Unsere ganze Zahl ist allgemein durch die Funktion

$$a + a_1 i + a_2 i i_1 + a_3 i i_1 i_2 + \ldots + a_n (i i_1 i_2 \ldots i_{n-1})$$

definirt, worin i, $i i_1$, $i i_1 i_2$ u. s. w. die Richtungskoeffizienten der neutralen Grössen des n-dimensionalen Grössengebietes und die Koeffizienten $a, a_1, a_2, \ldots$ ganze reelle Zahlen bezeichnen, sodass es sich immer um eine Aneinanderreihung ganzer Mengen neutraler Einheiten oder, geometrisch, um einen Vektor mit ganzen rechtwinkligen Koordinaten handelt.

Es steht Jedem frei, eine besondere Funktion mit einem besonderen Namen zu belegen; nur wäre es wünschenswerth, dass die Willkür der Benennung nicht zu Widersprüchen in der eigenen Theorie führte. Kummer und seine Nachfolger nennen die Funktion

$$f(\alpha) = a + a_1 \alpha + a_2 \alpha^2 + \ldots + a_{n-1} \alpha^{n-1}$$

worin α eine komplexe Wurzel n-ten Grades aus der Einheit, $\alpha, \alpha^2, \ldots \alpha^{n-1}$ mithin die $n-1$ verschiedenen Werthe von $\sqrt[n]{1} = e^{\frac{2\pi i}{n}}$ und die Koeffizienten $a, a_1, a_2, \ldots$ ganze reelle Zahl sind, eine komplexe ganze Zahl oder schlechthin eine ganze Zahl. (Vergl. Crelle's Journal Band 35 Nr. 15 und 16, Bachmann's Kreistheilung 18. Vorlesung, u. A.) An höhere Zahlengebiete als das zweidimensionale wird hierbei nicht gedacht und kann nicht gedacht werden, weil nur für das zweidimensionale Gebiet die n-te Wurzel der Einheit n Werthe (im dreidimensionalen Gebiete schon n^2, im vierdimensionalen Gebiete n^3 Werthe u. s. w.) hat, ausserdem aber die Behandlung der Funktion $f(\alpha)$ nach den Regeln der gewöhnlichen Multiplikation, Division und Potenzirung nach dem Obigen unzulässig sein würde und die daraus gezogenen Resultate ganz falsch sein würden. Wir haben es daher bei den letzteren Funktionen und Operationen nur mit gewissen Formen und Operationen in der zweidimensionalen Zahlenebene oder mit Grössen zu thun, welche stets durch eine gewöhnliche komplexe Zahl von der Form $a + bi$ gedeckt werden. (Die Beschränkung auf den Fall, wo n eine Primzahl ist, welche sich die Autoren gewöhnlich auferlegen, ist etwas Nebensächliches).

Beispielsweise ist für $n = 4$ $3 + 5e^{\frac{2\pi}{4}i} = 3 + 5i$ eine ganze, $-2{,}5 + 0{,}866\,i$ aber eine unganze Zahl. Für $n = 3$ ist $2 + 5e^{\frac{2\pi i}{3}} + 4e^{\frac{4\pi i}{3}} = -2{,}5 + 0{,}866\,i$ eine ganze Zahl. Einunderselbe Grössenwerth erscheint also bald als ganze, bald als unganze Zahl, und zwar ist diese Gemeinschaft kontradiktorisch entgegengesetzter Eigenschaften nicht etwa ein singuläres, sondern ein generelles Vorkommen, eine nothwendige Folge der Definition. Ob sich Diess rechtfertigen lässt, scheint fraglich; übrigens betrifft es nur die Terminologie, also etwas Äusserliches: wenn man $f(\alpha)$ eine ganze Kummersche Funktion nennte, wäre dieser Übelstand beseitigt, und man hätte es mit der Theorie einer besonderen Funktionsform zu thun, welche mit dem Wesen einer ganzen Zahl nur eine nebensächliche Beziehung, nämlich die Zusammensetzung aus ganzen Vielheiten der verschiedenen Potenzen einer an sich unganzen Grösse α, gemein hat.

Eine solche Untersuchung, geistreich geführt, kann manches interessante Zahlengesetz enthüllen, wie die schönen Arbeiten von Kummer und Anderen thatsächlich beweisen: man hat sich aber durch gewisse Resultate verleiten lassen, die Generalisirung der Zahlform, welche in der Zulassung aller beliebigen Wurzelgrade n besteht, für eine Generalisirung der Dimensität des Grössengebietes zu halten und demzufolge in jenen Gesetzen allgemeinere Gesetze höher dimensionirter Gebiete zu erblicken. Hierin liegt ein entschiedener Irrthum; die fraglichen Untersuchungen bewegen sich, wie aus dem Erwähnten unzweideutig hervor-

geht, ausschliesslich in der Zahlenebene der komplexen Zahlen und liefern die Gesetze gewisser ebenen, durch die Funktion $f(\alpha)$ vertretenen Gebilde; sie treten nicht in den dreidimensionalen Zahlenraum hinaus.

Als ein besonderes ebenes Gebilde nimmt die Funktion $f(\alpha)$ selbstredend ein gewisses Interesse in Anspruch: sie hat auch eine beachtenswerthe geometrische Bedeutung, welche darin besteht, dass durch sie eine Grösse sich als Summe ganzer schiefwinkliger Koordinaten darstellt, deren Axen sich, wenn $\alpha = e^{\frac{2\pi}{n}i}$ ist, unter den Winkeln $0, \frac{2\pi}{n}, \frac{4\pi}{n}, \frac{6\pi}{n}, \ldots \frac{2(n-1)\pi}{n}$ gegen die reelle Grundaxe neigen, die Funktion $f(\alpha)$ stellt also den Vektor oder die letzte Seite eines ebenen Polygons von $n+1$ Seiten dar, welche den genannten Axen parallel laufen und ganze Vielfache der Längeneinheit enthalten. Wenn man diese Beschränkung der Seitenlängen auf ganze Vielfachen der Längeneinheit fallen lässt, ist

$$f(\alpha) = x + x_1 \alpha + x_2 \alpha^2 + \ldots + x_{n-1} \alpha^{n-1}$$

die allgemeine Formel für einen solchen Vektor, indem $x, x_1, x_2, \ldots x_{n-1}$ die reellen, aber sonst beliebigen ganzen, gebrochenen oder irrationalen positiven oder negativen Werthe seiner Koordinaten bezeichnen. Diese Auffassung scheint der Kummerschen Funktion die Bedeutung einer Verallgemeinerung der Formeln der analytischen Geometrie, durch welche Vektoren mittelst recht- oder schiefwinkliger Koordinaten dargestellt werden, zu ertheilen: Diess ist jedoch nur in gewisser Hinsicht der Fall. Die geometrische Auffassung lässt für ein Koordinatensystem in der Ebene nur zwei, für ein System im Raume nur drei, überhaupt für irgend ein System nur eine bestimmte, seiner Dimensität entsprechende Anzahl von Axen zu: die Kummersche Formel dagegen verlangt für ein ebenes System (und überhaupt für jedes System) die volle, sonst aber beliebig wählbare Anzahl von n Koordinatenaxen. Hierdurch wird die Darstellung einer Grösse mittelst der Funktion $f(\alpha)$ eine völlig unbestimmte: man kann eine gegebene Grösse in unendlich verschiedener Weise, d. h. mit unendlich verschiedenen Koeffizienten $x, x_1, x_2, \ldots$ in der Form des Polynoms $x + x_1 \alpha + x_2 \alpha^2 + \ldots$ darstellen, wovon man sich überzeugt, wenn man sowohl die gegebene Grösse, als dieses Polynom in seinen reellen und imaginären Bestandtheil auflös't und beide bezw. einander gleich setzt. Ist $n > 2$; so erhält man hierdurch zwei Gleichungen ersten Grades zwischen n Unbekannten $x, x_1, x_2, \ldots x_{n-1}$, welchen durch unendlich viel reelle Werthe dieser Unbekannten genügt werden kann.

Aber auch in der Form der eigentlichen Kummerschen Zahl, nämlich unter der Bedingung, dass $x, x_1, x_2, \ldots$ lauter ganze reelle Werthe haben, bleibt der Ausdruck für $f(\alpha)$, wenn er einen gegebenen Werth haben soll, völlig unbestimmt. Denn angenommen, die Funktion $f(\alpha) = a + a_1 \alpha + a_2 \alpha^2 + \ldots + a_{n-1} \alpha^{n-1}$ habe einen gegebenen Werth. Die Summe $1 + \alpha + \alpha^2 + \ldots + \alpha^{n-1}$ ist $= \frac{\alpha^n - 1}{\alpha - 1}$ und da $\alpha^n = 1$ ist, gleich null. Demzufolge ist auch für jeden Werth von x

$x + x\,u + x\,u^2 + \ldots + x\,u^{n-1} = 0$. Addirt man diese Gleichung zu der gegebenen; so kömmt

$$(a + x) + (a_1 + x)\,u + (a_2 + x)\,u^2 + \ldots + (a_{n-1} + x)\,u^{n-1} = f(u)$$

Man sieht, dass die Funktion $f(u)$ ihren Werth nicht ändert, wenn man alle ihre Koeffizienten um denselben ganz beliebigen Betrag x verändert, dass also eine Grösse in unendlich verschiedener Weise als Kummersche ganze Zahl dargestellt werden kann. Dieses Resultat hat einen leicht verständlichen geometrischen Sinn. Stellt man z. B. für $n = 5$ durch die Richtungen OX, OX_1, OX_2, OX_3, OX_4 5 schiefwinklige Koordinatenaxen und durch OA, AA_1, A_1A_2, A_2A_3, A_3A_4 fünf diesen Axen parallele Linien dar; so ist der vom Anfangspunkte O nach dem Endpunkte A_4 des Zuges $OAA_1A_2A_3A_4$ führende Vektor $OA_4 = f(u) = (OA) + (AA_1) + (A_1A_2) + (A_2A_3) + (A_3A_1)$. Verlängert man alle Seiten des Zuges $OAA_1A_2A_3A_4$ um irgend eine bestimmte Länge AB; so wird der Endpunkt des neuen Zuges $OBB_1B_2B_3B_4$ mit dem Endpunkte A_4 des früheren zusammenfallen (weil die Seitendifferenzen ein geschlossenes regelmässiges Fünfeck bilden). Durch eine besondere Disposition über die Koeffizienten kann man allerdings den vorstehenden Ausdruck auf eine einzige bestimmte Form, die sogenannte Normalform, bringen; allein, das betrifft nur die Definition der Funktion $f(u)$, nicht das Materielle der Sache: die ganzzahligen Koeffizienten des Polynoms, welches einen bestimmten Werth haben soll, also die Koordinaten einer fest bestimmten Grösse in diesem Koordinatensysteme können unendlich verschiedene Werthe annehmen.

Hierzu kömmt, dass auch die Normalform, worunter eine Form zu verstehen ist, welche die Darstellung einer gegebenen Zahl als Funktion $f(u)$ nur in einziger Weise zulässt, durchaus keine fest bestimmte Form ist, dass vielmehr die letztere Forderung durch verschiedene Bedingungen erfüllt werden kann. Kummer spricht überhaupt nicht von einer Normalform, und Bachmann's Festsetzungen über diese Form in der 6. Vorlesung Nr. 3 sind nicht die einzig möglichen. Man kann nach Vorstehendem immer dafür sorgen, dass der erste Koeffizient a in der Funktion $f(u)$ gleich null wird: Diess ergiebt die Bachmannsche Normalform. Man kann aber statt des ersten den letzten Koeffizienten a_{n-1} oder irgend einen anderen gleich null werden lassen, man kann auch bestimmen, dass er gleich 1 werde oder dass er einen beliebigen bestimmten Werth annehme. Jede dieser Bedingungen entspricht einer Normalform.

Unsere polydimensionale oder polyplexe Zahl unterscheidet sich hiernach von der Kummerschen wesentlich dadurch, dass erstere nur eine einzige Darstellung einer gegebenen Grösse mittelst Koordinaten, letztere aber unendlich viel verschiedene Darstellungen oder eine Darstellung mittelst unendlich verschiedener Koordinaten bei gegebenem Koordinatensysteme zulässt. Diess gilt für unsere polyplexe Zahl jeden Gebietes und würde auch für die Kummersche Zahl jeden Gebietes gelten, wenn hier überhaupt von einem mehr- als zweidimensionalen Gebiete die Rede sein könnte, was jedoch nicht möglich ist, da die Rechnungs-

regeln des zweidimensionalen Gebietes die Grundlage der Kummerschen Theorie bilden und diese Regeln nicht ohne Weiteres auf höhere Gebiete Anwendung finden. Die Einzigkeit der Form, welche unserer polyplexen Zahl zukömmt, und die Unabhängigkeit ihrer Form von dem Gebiete, in dem man sich bewegt, verleihet ihr in hervorragendem Maasse den Charakter der natürlichen Zahlform, wogegen die Kummersche als eine der vielen Spezialitäten künstlicher Zahlformen erscheint. Man kann daher unsere ganze Zahl, gegenüber anderen Funktionen mit ganzen Koeffizienten, als die natürliche ganze Zahl ansehen.

Wir heben noch hervor, dass die stetige Variation der Koeffizienten der Kummerschen Funktion zwar eine Variation nach n Axen ist, dass jedoch alle diese Axen in der zweidimensionalen Zahlenebene liegen, also nicht im Neutralitätsverhältnisse zueinander stehen und dass demzufolge eine Variation nach drei Axen dieser Art nicht für eine Variation nach den drei Axen des Raumes gehalten werden darf.

2) Dass eine Funktion, welche eine bestimmte Grösse in verschiedener Weise darstellen kann, wesentlich andere Resultate hinsichtlich ihrer Theilbarkeit durch gleichartige Funktionen ergeben muss, als eine Funktion, welche eine bestimmte Grösse nur in einziger Weise darstellt, ist begreiflich. Die Kummersche Theorie führt zu der Annahme sogenannter idealer Zahlen, insbesondere idealer Primfaktoren, von welchen unsere Theorie Nichts weiss. Die idealen Zahlen sind den realen oder wirklichen (reellen und komplexen) Zahlen als unwirkliche Zahlen gegenübergestellt; sie sind nicht direkt durch bestimmte Grundeigenschaften, sondern indirekt durch gewisse entfernte Wirkungen, welche sie als Faktoren hervorbringen sollen, ohne dass diese Wirkungen durch mathematische Gesetze zu konstruiren wären, definirt; man kann daher eine ideale Zahl nicht schreiben oder formuliren, sondern muss wie an ein im Verborgenen ruhendes Geheimniss an sie glauben. Unwirkliche Dinge, welche nicht darstellbar sind und auch nicht wirklich werden können, sind unmögliche Dinge, und wenn sie in ihrem Wesen, ihren Grundeigenschaften, ihren unmittelbaren Beziehungen zu den Basen der Grundoperationen nicht erkennbar sind, wenn ihre Entstehung aus diesen Basen durch Grundoperationen nicht gezeigt werden kann, sind sie überhaupt keine Grössen, sondern Fiktionen. Ideale ganze Zahlen giebt es nicht.

In der That, nach Kummer's Theorie hat die ganze Zahl $f(\alpha)$ dann wirkliche ganze Faktoren, wenn es ganze Zahlen wie $f_1(\alpha)$, $f_2(\alpha)$, $f_3(\alpha)$ u. s. w. giebt, deren Produkt ein mit $f(\alpha)$ übereinstimmendes Resultat liefert: wenn es aber solche Faktoren nicht giebt, wird dennoch von idealen Faktoren gehandelt, welche unter Umständen in $f(\alpha)$ enthalten sein sollen. Ohne Frage wird jede mögliche Grösse des zweidimensionalen Gebietes, sie mag den Werth irgend welcher Funktion darstellen, in ihrem Endresultate durch eine komplexe Grösse $x + x_1 i$ gedeckt: demzufolge hat nicht nur die Kummersche Funktion $f(\alpha) = A + A_1 i$, sondern auch jede Zahl von gleicher Form, welche man als ihren Faktor ansehen will, einen äquivalenten komplexen Werth. Umgekehrt, lässt sich jede komplexe Zahl leicht in die Form einer Kummerschen Funktion mit

reellen, wennauch nicht immer ganzen Koeffizienten bringen. Hiernach hat man immer, wenn $b + b_1 i$, $c + c_1 i$ u. s. w. die äquivalenten Werthe beliebiger Funktionen $f_1(\alpha)$, $f_2(\alpha)$, $f_3(\alpha)$ u. s. w. sind, deren Produkt den äquivalenten Werth der Funktion $f(\alpha)$ haben soll, die Gleichung

$$(b + b_1 i)(c + c_1 i)(d + d_1 i) \ldots = A + A_1 i$$

worin A und A_1 durch die Koeffizienten b, b_1, c, c_1, d, d_1, ... leicht bestimmt werden können. Die Grössen A, A_1, b, b_1, c, c_1, ... sind unbedingt reelle, wennauch nicht ganze Zahlen. Das Produkt ganzer Kummerschen Funktionen ist immer, wie leicht zu erachten, eine ganze Kummersche Zahl: giebt es also keine ganze Zahl $f_1(\alpha)$, welche mit anderen ganzen oder unganzen Zahlen $f_2(\alpha)$, $f_3(\alpha)$ u. s. w. als Produkt die ganze Zahl $f(\alpha)$ erzeugt; so müssen alle Faktoren, welche möglicherweise das Produkt $f(\alpha)$ hervorbringen können, da dieselben, wenn sie überhaupt als mathematische Grössen existiren, den komplexen Grössen $b + b_1 i$, $c + c_1 i$, $d + d_1 i$ u. s. w. äquivalent sind und diese sich immer in die Form Kummerscher Funktionen bringen lassen, nothwendig Kummersche Funktionen mit unganzen Koeffizienten sein. Wenn aber der ideale Primfaktor eine Funktion mit unganzen Koeffizienten ist; so ist er überhaupt keine Kummersche ganze Zahl, er existirt also nicht, und die Annahme seiner Existenz ist ein Widerspruch gegen die Voraussetzung, auf welcher die Vorstellung einer ganzen Zahl beruht.

Kummer erkennt die Unwirklichkeit der idealen Zahl in den zitirten beiden Abhandlungen namentlich auf S. 319, 324, 352, 353 mit deutlichen Worten an, wiewohl die Vergleichung des Idealen mit dem Imaginären auf S. 354 und mit den nicht isolirbaren chemischen Elementen auf S. 360 mit der Unwirklichkeit nicht recht vereinbar ist und vielleicht auch nur ein Gleichniss zu etwas bis dahin Unerklärtem sein soll. Zu solchen bildlichen Ausschmückungen dürfte auch der auf S. 320 enthaltene Hinweis auf die Unwirklichkeit oder die ideale Existenz der Sehne zweier sich nicht schneidenden Kreise zu rechnen sein. Bachmann findet übrigens diese Analogie so überzeugend, dass er geradezu erklärt, „im Grunde sei bei dem idealen Primfaktor nirgends etwas Imaginäres, als in der Bezeichnung“. Diese Meinung vermag ich nicht zu theilen, halte vielmehr die fragliche Analogie für unzutreffend, und zwar aus folgenden Gründen.

Die Gleichung des Kreises $y = \sqrt{a^2 - x^2}$ oder, wie dieselbe nach den Prinzipien des Situationskalkuls zu schreiben ist,

$$r = x + \sqrt{a^2 - x^2}\,\sqrt{-1}$$

stellt für reelle Werthe von x nicht allein die mit dem Radius a beschriebene Kreislinie, sondern auch den nach beiden Seiten ins Unendliche verlängerten, in der Richtung der Grundaxe liegenden Durchmesser dar. Für Werthe von x, welche $< a$ sind, gehören die beiden Endpunkte des gemeinschaftlichen Vektors der Kreislinie an; für grössere Werthe von x gehören sie dem verlängerten Durchmesser an. Ein zweiter Kreis, vom Radius a', dessen Mittelpunkt in der Grundaxe in der Entfernung c liegt, nebst seinem Durchmesser wird durch die Gleichung

$$r' = x' + \sqrt{a'^2 - (x' - c)^2}\,\sqrt{-1}$$

dargestellt. Die beiden Funktionen r und r' werden einander gleich, wenn $x = x'$ den Werth $\frac{a^2 - a'^2 + c^2}{2c}$ annimmt. Für diesen Werth von x fallen also immer zwei Punkte der durch r und r' dargestellten Linienzüge zusammen. Ist dieser Werth von $x < a$; so liegen die zusammenfallenden Punkte in den beiden Kreislinien und bilden eine auf der Axe normal stehende Sehne: ist dagegen der fragliche Werth von $x > a$; so liegen die zusammenfallenden Punkte in den durch die Funktionen r und r' ebenfalls dargestellten verlängerten Durchmessern der beiden Kreise und bilden eine in die Grundaxe fallende Sehne. Immer aber haben die beiden zusammenfallenden Punkte und ihre Verbindungslinie, welche stets eine gemeinschaftliche Sehne der durch die beiden Gleichungen dargestellten Linienzüge ist, eine wirkliche Existenz.

Läge der Mittelpunkt des zweiten Kreises nicht in der Grundaxe, sondern im Endpunkte des Vektors $m + n\sqrt{-1}$; so wäre die Gleichung dieses Kreises $r' = x' + \left\{ n + \sqrt{a'^2 - (x' - m)^2} \right\} \sqrt{-1}$. Die Beschränkung der Werthe der Abszisse x in der Gleichung des Kreises auf reelle Werthe ist eine ganz willkürliche: wenn man dieselbe aufhebt und für x sowohl reelle wie komplexe Werthe, also überhaupt zweidimensionale Werthe zulässt; so stellt die Funktion $r = x + \sqrt{a^2 - x^2}\sqrt{-1}$ unendlich viel Linienzüge in der Grundebene dar. Das Nämliche gilt von der letzteren Funktion r', und auch für diese allgemeinere Voraussetzung haben die beiden Funktionen r und r' für einen bestimmten Werth von x zwei Werthe miteinander gemein, welche zwei bestimmten Punkten der Grundebene entsprechen; die gemeinschaftliche Sehne der beiden durch jene Funktionen dargestellten Raumgebilde existirt daher immer in der Wirklichkeit, die idealen Primfaktoren dagegen existiren nicht.

Zu welchen eigenthümlichen Vorstellungen die Theorie der idealen Zahlen nöthigt, lehrt folgender Satz. Aus der Gleichung

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = (x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{p-1})$$

worin α die komplexe Wurzel p-ten Grades aus der Einheit 1 bezeichnet, wird für $x = 1$ die Formel

$$p = (1 - \alpha)(1 - \alpha^2) \ldots (1 - \alpha^{p-1})$$

also der im Sinne der Kummerschen Theorie ganz richtige Satz abgeleitet, dass jede reelle Primzahl p in $p - 1$ wirkliche komplexe Faktoren zerlegbar sei, welche Kummersche ganze Zahlen sind. Sodann wird weiter deduzirt, dass jeder dieser Faktoren sich von dem anderen nur durch einen Faktor $E(\alpha)$ unterscheide, welcher den Werth einer Einheit habe, indem

$$1 - \alpha^n = (1 - \alpha) \cdot E(\alpha)$$

sei (vgl. Bachmann S. 256 der Kreistheilung und Kummer S. 348 von Crelle's Journal). Da dieser Einheitswerth

$$E(\alpha) = \frac{1 - \alpha^n}{1 - \alpha} = 1 + \alpha + \alpha^2 + \ldots + \alpha^{n-1}$$

ist; so stellt derselbe für die verschiedenen Werthe von $n = 1$ bis n

$= p - 1$ geometrisch die verschiedenen von dem Anfangspunkte A des regelmässigen p-eckes $A A_1 A_2 A_3 \ldots A_{n-1}$ gezogenen Diagonalen $A A_1$, $A A_2$, $A A_3$, $\ldots A A_{n-1}$ und für $n = p$ den Nullwerth (oder geometrisch den Punkt $A A$) dar. Alle diese Linien von verschiedener Länge und Richtung sollen nun Einheiten repräsentiren; sie haben sowohl geometrisch, als auch arithmetisch wirkliche Existenz und sind sogar nach ihrer Form $1 + \alpha + \alpha^2 + \ldots$ Kummersche wirkliche ganze Zahlen. Hiernach müssen der Theorie zu Liebe ganze Zahlen, welche nicht den Einheitswerth haben und welche auch nicht in jeder beliebigen ganzen Zahl aufgehen, die Rolle von fingirten Einheiten übernehmen, ja selbst die Null muss konsequenter Weise diesen Dienst leisten.

Ich erkenne die Genialität Kummer's, sowie die Wichtigkeit und Tiefe seiner Untersuchungen vollkommen an, kann jedoch dem Begriffe des idealen Faktors nicht die Bedeutung einer Grösse, sondern nur die Bedeutung eines Hülfsbegriffes zuschreiben, welcher geeignet ist, eine Klasse interessanter Beziehungen zwischen den Wurzeln der höheren Gleichungen und Kongruenzen in kurzer Weise zum Ausdruck zu bringen. Als Hülfsbegriff ist der ideale Faktor thatsächlich eine ideale, d. h. eine unwirkliche, nicht existirende Grösse, welche auch kein Analogon im anschaulichen Raume hat, welcher jedoch die Fähigkeit, in Gemeinschaft mit anderen ideellen Faktoren reelle Grössen als Multiplikationseffekte hervorzubringen, zugeschrieben wird, ohne dass sich zeigen lässt, wie Diess geschieht. Man postulirt also gewissermaassen zwei Eigenschaften: eine ideale Existenz und eine ideale Kraft oder Wirksamkeit, etwa so, als wenn ich einer Welt von möglichen Objekten a, b, ... oder einer möglichen Welt eine Welt von unmöglichen Objekten α, β, ... oder eine unmögliche Welt gegenüberstelle und den letzteren Objekten die Kraft zuschreibe, einem Objekte, worauf es wirkt, die Möglichkeit zu entziehen oder dasselbe unmöglich zu machen. Unter dieser Hypothese wird die Zusammenwirkung zweier möglichen Objekte a und b wieder ein mögliches Objekt ab, die Zusammenwirkung eines möglichen und eines unmöglichen Objektes a und α sowohl in der Form $a \times \alpha$ als Wirkung von α auf a, als auch in der Form $\alpha \times a$ als Wirkung von a auf α ein unmögliches Objekt, die Zusammenwirkung zweier unmöglichen Objekte α und β aber durch Aufhebung der Unmöglichkeit des α durch die Wirkung des β ein mögliches Objekt ergeben. Solche logischen Allgemeinheiten können in der formalen Logik der Begriffe ihren Platz finden; die Mathematik jedoch, welche eine logische Behandlung der konkreten Grössen oder der anschaulichen, wirklichen Objekte ist, kann keine generellen, sondern nur durch konkrete Gesetze konstruirbare Möglichkeiten zulassen.

Mir scheint, dass Kummer in der Abhandlung 16 in Crelle's Journal auf S. 355 gewissermaassen selbst den Beweis von der Unmöglichkeit idealer Primfaktoren führt, indem er zu dem Resultate gelangt, dass jede ideale Zahl die Eigenschaft hat, dass eine gewisse ganze Potenz derselben eine wirkliche (Kummersche) Zahl sei, dass sich also jede ideale Zahl als eine Wurzel aus einer wirklichen (Kummerschen) Zahl darstellen lasse. Der Wurzelbegriff schliesst im Allgemeinen sowohl die Ganzzahligkeit des Resultates, als auch die Darstellbarkeit

durch ein Polynom mit ganzen Potenzen einer bestimmten Einheitswurzel α aus, und der vorstehende Satz lehrt zugleich, dass der ideale Primfaktor eine wirkliche Kummersche Zahl mit irrationalen Koeffizienten, also keine ganze Zahl ist.

Wenn man nun auch der idealen Zahl alle Rechte eines Hülfsbegriffes einräumt; so muss man doch noch eines schwer wiegenden Bedenkens gegen die damit begründeten Sätze der Theilbarkeit erwähnen. Unverkennbar lässt sich jede gegebene gemeine reelle oder komplexe ganze Zahl durch irgend eine Kummersche ganze Zahl $f(\alpha)$ darstellen, d. h. es giebt einen Exponenten n, welcher Diess ermöglicht: allein, keineswegs lässt sich durch die ganze Funktion $f(\alpha)$ mit gegebenem Exponenten n jede beliebige gemeine ganze Zahl darstellen. Nimmt man z. B. $n = 3$; so ist $f(\alpha) = a + a_1 e^{\frac{2\pi i}{3}} + a_2 e^{\frac{4\pi i}{3}}$ $= a - \frac{1}{2}(a_1 + a_2) + 0{,}866\,(a_1 - a_2)\,i$. Sollen nun die Koeffizienten a, a_1, a_2 ganze reelle Werthe haben; so kann durch $f(\alpha)$ durchaus keine gemeine komplexe ganze Zahl $b + b_1 i$, auch noch nicht einmal eine imaginäre ganze Zahl $b_1 i$ dargestellt werden. Zu einem gegebenen Exponenten n gehören also nur gewisse ganze Zahlen des gemeinen Zahlengebietes, welche eine besondere Klasse bilden; im Allgemeinen sind die Zahlen der einen Klasse nicht durch die Funktion einer anderen Klasse darstellbar. Die Sätze über die Theilbarkeit der ganzen Zahlen und über die Einzigkeit der Zusammensetzung aus idealen Primfaktoren betreffen daher immer nur eine gewisse Klasse, durchaus nicht alle ganzen Zahlen aller möglichen Klassen, sie sind also keine allgemeinen Gesetze für das gesammte Zahlengebiet. Für $n = 1$ und auch für $n = 2$ erscheint das Gebiet der reellen Zahlen als eine Klasse, für $n = 4$, was $f(\alpha) = a + a_1 i + a_2 i^2 + a_3 i^3 = (a - a_2) + (a_1 - a_3) i$ ergiebt, erscheint das Gebiet der reellen und komplexen Zahlen als eine Klasse; für eine unpaare Primzahl n fällt jedoch keine gemeine komplexe Zahl in die Klasse. Für das zweidimensionale Gebiet stimmen die Gesetze der idealen Primfaktoren mit denen der wirklichen überein; für dieses Gebiet decken sie also über die Theilbarkeit der Zahlen nichts Anderes auf, als was in den gewöhnlichen Zahlengesetzen liegt, und für die höheren Kummerschen Zahlformen gelten sie immer nur für die dem Exponenten n entsprechende Formenklasse.

§. 19. Die algebraische Zahl.

1) Indem Dedekind zur Begründung der Theorie der algebraischen ganzen Zahlen in der Kummerschen Funktion $f(\alpha)$ an die Stelle einer komplexen Wurzel α der Gleichung $x^n - 1 = 0$ eine Wurzel ϑ der irreduktibelen (unzerlegbaren) algebraischen Gleichung $x^n + b_1 x^{n-1} + \ldots + b_n = 0$ setzt und die Funktion

$$\varphi(\vartheta) = a + a_1 \vartheta + a_2 \vartheta^2 + \ldots + a_{n-1} \vartheta^{n-1}$$

deren Koeffizienten a, a_1, $\ldots$ a_{n-1} ganze reelle Zahlen sind, als ganze Zahl des durch $\varphi(\vartheta)$ mit allgemeinen Koeffizienten repräsentirten ge-

sammten Zahlenkörpers definirt (vgl. Supplement XI zur dritten Auflage der von Dedekind herausgegebenen Vorlesungen von Dirichlet, sowie auch die Theorie der algebraischen Funktionen von Dedekind und Weber in Crelle's Journal für Mathematik, Band 92), entfernt er sich noch weiter von der Vorstellung der natürlichen ganzen Zahl, verallgemeinert aber andererseits den Begriff der Kummerschen ganzen Zahl, sodass die letztere als ein Spezialfall der ersteren erscheint und daher möglicherweise die Kummerschen idealen ganzen Zahlen, welche in der Form der Funktion $f(\alpha)$ irrationale Zahlen sein würden, als algebraische ganze Zahlen reproduziren könnte. In der That, irgend eine Wurzel ϑ einer gegebenen Gleichung n-ten Grades hat für eine Primzahl n die Form

$$\vartheta = A + \alpha \sqrt[n]{\eta_1} + \alpha^2 \sqrt[n]{\eta_2} + \ldots \alpha^{n-1} \sqrt[n]{\eta_{n-1}}$$

Hierin bezeichnen $\eta_1, \eta_2, \ldots \eta_{n-1}$ die $n-1$ Wurzeln einer Gleichung vom $(n-1)$-ten Grade, deren Koeffizienten von den Koeffizienten der gegebenen Gleichung oder von den Wurzeln dieser Gleichung abhängen. Die Grössen $\alpha, \alpha^2, \ldots \alpha^{n-1}$ haben dieselbe Bedeutung der Einheitswurzeln wie in der Kummerschen Funktion, und $nA = \vartheta_1 + \vartheta_2 + \vartheta_3 + \ldots + \vartheta_n$ ist die Summe der n Wurzeln der gegebenen Gleichung. Hiernach kann die Wurzel ϑ und jede Potenz davon in die Form einer Kummerschen Funktion gestellt werden, deren Koeffizienten gewisse Funktionen der n Wurzeln einer Gleichung n-ten Grades sind: die ganze algebraische Zahl ist daher eine unganze, insbesondere eine irrationale Kummersche Zahl.

Diese Beziehung zwischen den Funktionen $f(\alpha)$ und $\varphi(\vartheta)$ könnte nun denkbarer Weise die Erklärung dafür enthalten, dass in Dedekind's Theorie der ideale Primfaktor keine Rolle spielt, indem die algebraischen Primfaktoren, welche Kummerschen Funktionen mit irrationalen Koeffizienten äquivalent sind, wirkliche algebraische ganze Zahlen sein könnten. Erwägt man jedoch, dass, wenn man in der Theorie der algebraischen Zahlen für ϑ die Wurzel der Gleichung $x^n - 1 = 0$ nimmt, die algebraische Zahl mit der Kummerschen Zahl und der algebraische Primfaktor mit dem idealen Primfaktor übereinstimmen muss, dass also, wenn ersterer eine wirkliche Zahl wäre, auch letzterer eine solche sein müsste; so darf man den Schluss ziehen, dass auch die algebraischen Primfaktoren keine Wirklichkeit haben, d. h. dass sie keine ganzen, sondern im Allgemeinen irrationale algebraische Zahlen sein werden. Ganze Primfaktoren, aus welchen die übrigen Zahlen eines Systems auf einzige Weise zusammengesetzt wären, giebt es daher auch unter den algebraischen ganzen Zahlen nicht. Ich glaube, dass diese Ansicht auch von dem Verfasser der Theorie dieser Zahlen getheilt wird: die Worte auf S. 505 ff. des §. 167 des erwähnten Supplementes XI dürften diese Ansicht deutlich bekunden; ausserdem würde sich die entgegengesetzte Ansicht doch wohl an irgend einer Stelle durch die Angabe eines echten Primfaktors, wenn es einen solchen gäbe, ausgesprochen haben. Beispiele, wie das auf S. 507, welche unzerlegbare algebraische Zahlen wie $\alpha = 2$, $\beta = 3$, $\mu = 1 - \vartheta$, $\nu = 1 + \vartheta$ anführen, die trotz der Unzerlegbarkeit in algebraische ganze Zahlen, doch keine echten

Primzahlen sind, dienen nicht allein dazu, die Unwirklichkeit der echten Primfaktoren zu konstatiren, sondern können auch leicht dazu verwandt werden, um zu zeigen, dass alle Faktoren von der generellen Form $\varphi(\vartheta)$, in welche jene Zahlen zu zerlegen sind, irrationale algebraische Zahlen sind.

Die vier Zahlen $2, 3, 1-\vartheta, 1+\vartheta$ gehören nämlich dem Körper zweiten Grades an, welcher aus einer Wurzel der Gleichung $\vartheta^2 + 5 = 0$ gebildet ist. Da hiernach $\vartheta = \sqrt{-5}$ ist; so ist das Produkt der beiden Zahlen 2 und 3 allerdings gleich dem Produkte der beiden Zahlen $1-\vartheta$ und $1+\vartheta$, nämlich gleich 6: die Zahl 6 lässt sich also auf zwei verschiedene Weisen in Faktoren zerlegen, welche doch als algebraische ganze Zahlen unzerlegbar sind. Hiernach spielen die Zahlen $2, 3, 1-\vartheta, 1+\vartheta$ nicht die Rolle echter Primfaktoren, sondern geben der Vermuthung Raum, dass sie selbst aus echten Primfaktoren bestehen. Hätten nun solche Faktoren die allgemeine Form der Funktion $\varphi(\vartheta) = a + a_1\vartheta$; so müsste die Zahl 2, wenn einer ihrer Primfaktoren $a + a_1\vartheta$ wäre, gleichviel, wie viel Primfaktoren sie sonst noch enthalten mag, da sich deren Produkt immer zu einer algebraischen Funktion zusammensetzt, das Produkt zweier algebraischen Funktionen $a + a_1\vartheta$ und $b + b_1\vartheta$ sein; man müsste also $ab + a_1 b_1 \vartheta^2 + (ab_1 + a_1 b)\vartheta = 2$ oder

$$2 - ab + 5a_1 b_1 = (ab_1 + a_1 b)\sqrt{-5}$$

haben. Diese Gleichung ist durch reelle Koeffizienten a, a_1, b, b_1 nur erfüllbar, wenn zugleich $2 - ab + 5a_1 b_1 = 0$ und $ab_1 + a_1 b = 0$ ist, weil für solche Werthe die linke Seite eine reelle und die rechte Seite eine imäginäre Grösse darstellt. Die zweite dieser beiden Bedingungen erfordert $b_1 = -\frac{a_1 b}{a}$ und die erste nach Elimination von b_1 $a^2 b - 2a = -5a_1^2 b$, also nach Multiplikation mit b und Hinzufügung von 1 auf beiden Seiten $ab = 1 \mp \sqrt{1 - 5a_1^2 b^2}$. Diese Gleichung ist aber für ganze reelle Werthe von a und b unerfüllbar; denn b kann nicht gleich null sein, weil Diess entweder auch für b_1 oder für a den Nullwerth erfordern, die erste Annahme aber die Absurdität $2 = 0$ und die zweite Annahme die für ganze Werthe von a_1 und b_1 unmögliche Forderung $2 = -5a_1 b_1$ nach sich ziehen würde: ebenso wenig kann a_1 gleich null sein, weil Diess entweder $a = 0$ oder $b_1 = 0$, also im ersten Falle die Absurdität $2 = 0$ und im zweiten Falle die für ganze und von 1 und 2 verschiedene Werthe von a und b unmögliche Forderung $2 = ab$ ergeben würde. Kann aber weder b, noch a_1 gleich null sein; so kann die fragliche Gleichung offenbar durch ganze reelle Werthe von a, b, a_1 nicht erfüllt werden.

Wir behaupten auch, dass die Koeffizienten a, a_1, b, b_1 der beiden Faktoren von 2 keine ganzen komplexen Zahlen sein können. Denn setzt man $a = c + di$, $a_1 = c_1 + d_1 i$, $b = e + fi$, $b_1 = e_1 + f_1 i$; so zerfällt die gegebene Gleichung, wenn das Reelle dem Reellen und das Imaginäre dem Imaginären gleich gesetzt wird, in die beiden Gleichungen

$$2 - ce + df + 5(c_1 e_1 - d_1 f_1) = -(cf_1 + de_1 + c_1 f + d_1 e)\sqrt{5}$$
$$cf + dc - 5(c_1 f_1 + d_1 e_1) = -(ce_1 - df_1 + c_1 e - d_1 f)\sqrt{5}$$

Da diese Gleichungen durch lauter ganze reelle Werthe der Grössen c, d, c_1, d_1, e, f, e_1, f_1 offenbar nicht erfüllbar sind; so leuchtet ein, dass ein Faktor von 2, welcher die Form der Funktion $\varphi(\vartheta)$ hat, weder ganze reelle, noch ganze komplexe Koeffizienten haben kann, dass es also echte Primfaktoren unter den algebraischen Zahlen selbst dann nicht giebt, wenn man auch ganze komplexe Koeffizienten zulassen wollte.

Dass man jede Zahl stets in algebraische und ideale Faktoren mit unganzen Koeffizienten zerlegen kann, ist selbstverständlich: ich bezweifle auch nicht, dass, wenn man die Form dieser Koeffizienten an eine durch eine bestimmte Funktion ausgedrückte Bedingung knüpft, diese Bedingung von der Art sein kann, dass sie die Darstellung jeder möglichen Zahl nach dieser Form in einziger Weise gestattet, dass sie also jedes Produkt aus solchen Zahlen wieder in derselben Grundform erscheinen lässt, dass sie jedoch nur gewisse Zahlen (welche Produkte anderer sind) in Faktoren von jener Form zu zerlegen erlaubt, dass mithin das System der in dieser Grundform dargestellten Zahlen echte Primfaktoren enthält, aus welchen alle übrigen Zahlen in einziger Weise zusammengesetzt sind. Das komplexe Zahlensystem ist ein solches System; in demselben liegen alle Zahlen, welche nach den bisher von den Analytikern angewandten Gesetzen darstellbar und denkbar sind (die polydimensionalen Zahlen stehen ausserhalb der Sphäre dieser Gesetze); die komplexen Primzahlen sind echte Primfaktoren im Sinne dieses Systems: das System der Kummerschen Funktionen und das der algebraischen Zahlen ist jedoch ein solches System nicht, da die echten Primfaktoren keine ganzen algebraischen Zahlen sind, und die Form der unganzen Koeffizienten, welche der vorstehenden Bedingung genügen würde, nicht bestimmt ist, auch in der Theorie dieser Zahlen keine Begründung finden würde.

Hinsichtlich der Einzigkeit des Ausdruckes für eine bestimmte Grösse erlaube ich mir zu bemerken, dass die algebraische Funktion $\varphi(\vartheta)$ von der in §. 18 S. 219 erwähnten Unbestimmtheit der Koeffizienten, welche der Kummerschen Funktion anhaftet, frei ist. Denn wenn dieselbe Zahl durch zwei verschiedene Ausdrucke $a + a_1\vartheta + a_2\vartheta^2 + \ldots + a_{n-1}\vartheta^{n-1}$ und $c + c_1\vartheta + c_2\vartheta^2 + \ldots + c_{n-1}\vartheta^{n-1}$ darstellbar ist; so muss $(a - c) + (a_1 - c_1)\vartheta + \ldots + (a_{n-1} - c_{n-1})\vartheta^{n-1} = 0$ sein; die Grösse ϑ muss also nicht nur der Gleichung n-ten Grades, deren Wurzel sie ist, sondern auch einer niedrigeren Gleichung genügen, was durch die Vorbedingung, wonach jene Gleichung n-ten Grades irreduktibel sein soll, ausgeschlossen ist. Demnach kann die Kummersche Funktion nicht ohne Weiteres in die algebraische Zahl übergeführt werden; denn die Gleichung $x^n - 1 = 0$ ist nicht irreduktibel, sondern nach Ausscheidung der Wurzel 1 auf die Gleichung $x^{n-1} + x^{n-2} + \ldots + x + 1 = 0$ reduzirbar (eine komplexe Wurzel der ersten Gleichung, welche hier überhaupt in Betracht kömmt, ist auch die Wurzel einer Gleichung niedrigeren Grades). Die algebraische Zahl, welche aus der Gleichung n-ten Grades $x^n + x^{n-1} + x^{n-2} + \ldots + x + 1 = 0$ entspringt, ist daher die Kummersche Zahl, welche der Kreistheilungsgleichung $x^{n+1} - 1 = 0$ angehört.

Aus Vorstehendem erhellet, dass ein echter Primfaktor auch nicht durch die Form der algebraischen Zahl darstellbar ist, dass es also auch

in diesem System von Funktionen keine echten Primfaktoren giebt. Dedekind vermeidet auch den Begriff eines konkreten Primfaktors vollständig; indem er alle unendlich vielen, unter einem bestimmten Gesichtspunkte zusammengehörigen Zahlen in einen Inbegriff zusammenfasst, der ein Ideal heisst, und alsdann für die Multiplikation und Theilung solcher Ideale besondere Begriffe bildet, gelangt er zu der Vorstellung von Primidealen, welche nach der ihnen und ihren Wirkungen beigelegten Bedeutung in dem Bereiche der algebraischen Zahlen dieselbe Rolle spielen, wie die Primzahlen nach der ihnen und ihren Wirkungen zukommenden Bedeutung im Bereiche der reellen Zahlen.

Die Einführung der Primideale, sowie die Operation mit Zahlenklassen von unendlichem Inhalt wie bestimmten, begrenzten Grössen hat seinen guten Grund. Was wir in §. 18 Nr. 2 über die Begrenztheit der Tragweite der Kummerschen Funktion $f(\alpha)$ gesagt haben, gilt auch von der algebraischen ganzen Funktion $\varphi(\vartheta)$: durch einen bestimmten Werth von ϑ kann nur eine bestimmte Klasse von Zahlen dargestellt werden. Nimmt man beispielsweise für ϑ die Wurzel der Gleichung $\vartheta^2 + 5 = 0$, also $\vartheta = \sqrt{5}.i$; so ist, da jetzt $n = 2$ ist, durch die algebraische Funktion $\varphi(\vartheta) = a + a_1\vartheta = a + a_1\sqrt{5}.i$ keine gemeine komplexe ganze Zahl, noch nicht einmal eine imaginäre ganze Zahl darstellbar. Die Theorie der algebraischen Funktion kann daher ebenso wenig wie die der Kummerschen Funktion allgemeine, für das ganze Zahlengebiet geltende, sondern nur für bestimmte Klassen gültige Gesetze in Betreff der Theilbarkeit entwickeln. Nach der Definition von $\varphi(\vartheta)$ überzeugt man sich leicht, dass im Allgemeinen oder mit Ausnahme von Grenzfällen zwei Klassen, welche aus verschiedenen Werthen von ϑ entspringen, keine Zahl $\varphi(\vartheta)$ miteinander gemein haben, dass diese Klassen also das gesammte Zahlengebiet in getrennte Spezialgebiete absondern, dass sich daher, wenn man diese Spezialgebiete wie Ganze behandelt und den Begriff der Multiplikation und Division solcher Gebiete an entsprechende Definitionen knüpft, Beziehungen ergeben, in welchen gewisse Spezialgebiete die Rolle von Primidealen übernehmen, während gewisse andere als zusammengesetzte Ideale erscheinen. Diese Ideale existiren dann in der Wirklichkeit, allein sie sind unendliche Inbegriffe und tragen schon aus diesem Grunde nicht den Charakter ganzer Zahlen, bei denen Begrenztheit eine wesentliche Voraussetzung ist; ausserdem hat Das, was von den Idealen als ganzen Inbegriffen gilt, keine Bedeutung für die konkreten Bestandtheile dieser Inbegriffe oder für die ganzen Zahlen selbst; die Zerlegbarkeit der Ideale kann daher über die Zerlegbarkeit der Zahlen keinen Aufschluss geben.

Wir machen auch hier die Bemerkung, dass die Verallgemeinerung der Funktion $f(\alpha)$ zur Funktion $\varphi(\vartheta)$, welche in der Vertauschung der Wurzeln einer speziellen Gleichung n-ten Grades mit den Wurzeln einer allgemeinen Gleichung dieses Grades besteht, zwar eine freiere, aber doch immer nur eine an die zweidimensionale Zahlenebene gebundene Bewegung verstattet, dass die durch den Exponenten n bedingte Variabilität der als Koordinaten aufgefassten Glieder des Polynoms $\varphi(\vartheta)$ eine Variation nach n Richtungen der Grundebene, aber keinen Austritt aus dieser

Ebene in den eigentlichen Zahlenraum gestattet, dass mithin die an den geometrischen Raum erinnernden Ausdrücke wie Zahlenkörper vom Grade n nicht auf wirkliche Raumgebilde von n Dimensionen, sondern nur auf ebene Gebilde mit n Variationsrichtungen gedeutet werden können. Demzufolge darf auch aus den speziellen Gesetzen der algebraischen Zahlen nicht der Schluss gezogen werden, dass sie die Gesetze der Grössen aller Zahlengebiete oder der polyplexen Zahlen enthalten.

Die Meinungsverschiedenheit, in welcher ich mich mit dem Begründer dieser Theorie hinsichtlich der Ausdeutung der algebraischen Zahlen auf die soeben erwähnten allgemeinen Zahlengebiete befinde, hindert mich nicht, den Resultaten, welche in sehr interessanten Beziehungen dieser Zahlformen unter sich und zu den Wurzeln der höheren Kongruenzen bestehen, sowie überhaupt der geistreichen Durchführung jener Theorie volle Anerkennung zu zollen.

Übrigens gestatte ich mir noch die Bemerkung, dass, während die Theorieen der idealen und der algebraischen ganzen Zahlen, wie sie vorliegen, ihren Schwerpunkt in der Theilbarkeit der Zahlen suchen, es rathsam erscheinen dürfte, eben diese spezielle Anwendung als eine Nebensache in den Hintergrund treten zu lassen und die allgemeinen Zahlengesetze zum wesentlichen Gesichtspunkte zu nehmen, da zu jener speziellen Anwendung der grosse Apparat jener Theorieen nicht erforderlich und auch nicht wirkungsvoll genug ist, indem sowohl die Kummersche, als auch die algebraische Zahl keine allgemeine, sondern eine Klassenzahl ist, ferner der ideale Faktor keine wirkliche und das Primideal keine konkrete Zahl ist, wogegen durch die natürliche und ganz allgemeine polydimensionale Zahl die Frage der Theilbarkeit auf die einfachste Weise mit wirklichen konkreten Zahlen gelös't wird (§. 17 Nr. 7).

2) Kronecker erweitert in seinen „Grundzügen einer Theorie der algebraischen Grössen“ (Crelle's Journal für Mathematik, Band 92) den Begriff der algebraischen Grösse über Dedekind's Definition der algebraischen Zahl hinaus, indem er in §. 2 alle diejenigen Grössen, welche rationale Funktionen der Grössen R', R'', R''', ... (d. h. Funktionen mit ganzzahligen Koeffizienten) sind, als ein Rationalitätsbereich $(R', R'', R''', \ldots)$, die Grössen R', R'', R''', ... als die Elemente eines solchen Bereiches und jede Wurzel einer irreduktibelen Gleichung n-ten Grades, deren Koeffizienten dem Rationalitätsbereiche $(R', R'', R''', \ldots)$ angehören, eine algebraische Funktion n-ter Ordnung der Grössen $R', R'', R''', \ldots$, die n Wurzeln einunderselben Gleichung aber konjugirte algebraische Funktionen nennt. Eine ganze algebraische Funktion der Variabelen R oder eine ganze algebraische Grösse soll nach §. 5 eine solche sein, welche einer Gleichung genügt, in der der Koeffizient der höchsten Potenz von x gleich eins und jeder andere Koeffizient eine ganzzahlige Funktion der R, also eine Grösse des Bereiches $(R', R'', R''', \ldots)$ ist. Für den Fall $R = 1$ sollen die ganzen algebraischen Grössen auch ganze algebraische Zahlen heissen. Die Gleichungen, um welche es sich handelt, haben also nach §. 7 die allgemeine Form

$$x^n + R' x^{n-1} + R'' x^{n-2} + \ldots + R^{(n)} = 0$$

Unter dieser Verallgemeinerung des Begriffes der algebraischen Grösse umfasst natürlich einunddieselbe Funktion wegen der Variabilität der Elemente ein ganzes Bereich von konkreten Grössen; die Kroneckerschen Bereiche treten daher an die Stelle der Dedekindschen Körper mit erweiterten Eigenschaften. In dieser Form erscheinen jene Bereiche allerdings in dem äusseren Gewande konkreter Grössen, sind jedoch in Wahrheit ebenfalls unendliche Inbegriffe von Elementen. Was sie hierdurch an Anschaulichkeit als konkrete Ganze gewinnen, büssen sie andererseits in Folge der grösseren Verallgemeinerung an der Anschaulichkeit ihrer Eigenschaften ein, namentlich verflüchtigt sich an ihnen in noch höherem Grade, als an den Idealen die Eigenschaft der Theilbarkeit, auf welche sich eigentlich die ganze Theorie zuspitzt. Man muss sich jetzt schon als Theiler Grössen oder Funktionen gefallen lassen, welche in Bruchform auftreten. Der Begriff der Theilbarkeit und des gemeinschaftlichen Maasses erweitert sich in Kronecker's, sowie in Dedekind's und Kummer's Theorie immer mehr zu der Vorstellung einer gesetzlichen Gemeinsamkeit in gewissen Beziehungen. (Schon bei Dedekind heisst der Model $\mathfrak{a}$, nämlich das System von reellen oder komplexen, algebraischen oder transzendenten Zahlen, welche sich durch Addition, Subtraktion und Multiplikation reproduziren, durch den Model $\mathfrak{b}$ theilbar, wenn jede in $\mathfrak{a}$ enthaltene Funktion zugleich in $\mathfrak{b}$ enthalten ist, was, abgesehen von der Umkehrung des gemeinen Begriffes der Theilbarkeit, eine ganz andere Eigenschaft, als elementare Theilbarkeit durch Division ausdrückt, indem zwei Grössen $(\alpha_1 + \alpha_2 + \alpha_3 + \ldots)$ und $(\alpha_1 + \alpha_2 + \alpha_3 + \ldots) + (\beta_1 + \beta_2 + \beta_3 \ldots)$, welche den Bedingungen eines Models oder eines Körpers entsprechen, wohl das System $(\alpha_1 + \alpha_2 + \alpha_3 + \ldots)$ als Glied, aber nicht als Faktor gemein haben).

Das Gesetz wirklicher Theilbarkeit und das Wesen wahrhafter Primfaktoren wird hiernach auch nicht durch Kronecker's algebraische Grössen realisirt. Aber selbst die in diesem Grössenbereiche herrschenden Analogien, welche bei veränderter Bedeutung jenem Gesetze entsprechen, haben keine Gültigkeit für drei- und mehrdimensionale Grössen. Es findet sich auch bei Kronecker auf S. 94 der schon vorhin erwähnte Irrthum, welcher mit folgenden Worten ausgesprochen ist: „Ganz ähnlich wie die Linie der reellen Zahlen durch die laterale Einheit zur Ebene der komplexen Zahlen sich ausdehnt, wird ein Grössenbereich $(R', R'', R''', \ldots)$ durch die Unbestimmtheit der ganzen algebraischen Formen gewissermaassen auf seine Dimension erweitert." Eine solche Ähnlichkeit liegt durchaus nicht vor, und da die Mathematik nicht mit Bildern und Gleichnissen, sondern mit Grössen rechnet; so dürfte man wohl fragen: wo ist denn die Grösse, welche dem Grössenbereiche $(R', R'', R''', \ldots)$ ebenso fremd, neu, ungleichartig gegenübertritt, um dieselbe Wirkung auf dieses Bereich, nämlich seine Verwandlung zu einem dreidimensionalen Gebiete hervorzubringen, welche die laterale oder imaginäre Einheit $i = \sqrt{-1}$ auf das Bereich der reellen Zahlenreihe ausübt? Die Analytiker verschliessen ja dieser Grösse, nämlich der überimaginären Einheit $\sqrt{\div 1}$ oder vielmehr der mit dem Zeichen $\div$ (cominus)

ausgedrückten Grundanschauung hartnäckig den Eintritt in ihre Theorieen und suchen sich durch die diktatorische Deklaration, dass eine Variabilität nach n Richtungen, die doch nirgends anders als in dem von ihnen angenommenen und durch die definirten Operationen allein zugänglichen Bereiche, also nur in der komplexen Zahlenebene liegen können, eine Variabilität nach n wirklichen Dimensionen des absoluten Grössengebietes sei, über die mit den aufgewandten Mitteln absolut unübersteigbare Schranke hinwegzutäuschen.

3) Mir däucht, dass das Wesen einer algebraischen Grösse, worunter ich eine aus ganzen positiv reellen Zahlen durch die bestimmten oder begrenzten oder abschliessenden oder endlichen Grundoperationen, nämlich durch die Numeration, Addition, Multiplikation und Potenzirung, sowie ihre Gegensätze, die Denumeration, Subtraktion, Division und Wurzelausziehung erzeugbare Grösse verstehe, auf die natürlichste und zugleich allgemeinste Weise durch die Darstellung, welche ich davon in §. 19 der „Beiträge zur Theorie der Gleichungen" gegeben habe, zur Erkenntniss gebracht wird, und dass sich im Anschlusse daran das Wesen der transzendenten Grösse, worunter ich eine lediglich durch stetige Variation, resp. durch unendliche Prozesse, also vornehmlich durch die fünfte Grundoperation, nämlich die Integration mit ihrem Gegensatze, die Differentiation, erzeugbare Grösse verstehe, am deutlichsten durch die Betrachtungen in §. 20 jener Schrift enthülle.

§. 20. Die Quaternion.

Ganz anders wie über die Kummerschen, Dedekindschen und Kroneckerschen Zahlformen urtheile ich über die Hamiltonschen Quaternionen und überhaupt über die aus sogenannten Haupteinheiten zusammengesetzten Grössen: die Ersteren sind mathematisch gesetzliche Zahlengebilde, die Letzteren dagegen sind ungesetzliche Haufwerke von unverstehbaren Symbolen. Die spezielle Begründung dieses Urtheils unter näherer Nachweisung der in der Theorie der Quaternionen liegenden Prinzipienfehler, falschen Schlüsse und sonstigen Unrichtigkeiten findet sich in §. 2 meiner Schrift über die polydimensionalen Grössen; ich beschränke mich hier auf folgende Bemerkungen.

Der Grundgedanke bei der Zulassung einer Haupteinheit j, worunter irgend eine Wurzel der positiven Einheit 1 oder auch der negativen Einheit -1 (welche selbst eine zweite Wurzel der positiven Einheit ist) verstanden wird, besteht darin, dass man einer solchen Wurzel von bestimmtem Grade n, also der Grösse $\sqrt[n]{-1} = e^{\frac{\pi}{n}\sqrt{-1}}$ ausser den in der Algebra bereits nachgewiesenen n Werthen $e^{\frac{\pi}{n}\sqrt{-1}}, e^{\frac{3\pi}{n}\sqrt{-1}}, \ldots e^{\frac{(2n-1)\pi}{n}\sqrt{-1}}$ auch noch andere Werthe beilegen könne, und dass demzufolge $\sqrt{-1}$ nicht nur den gewöhnlich dafür genommenen Werth $e^{\frac{\pi}{2}\sqrt{-1}}$, sondern auch manchen anderen Werth j habe. Jeden dieser verschiedenen Werthe von j glaubt man durch die Bedingung hinreichend definirt zu haben, dass er

die Gleichung $x^2 = -1$ erfülle, eine Gleichung, welcher nun nicht zwei, sondern noch sehr viel andere Wurzeln zugeschrieben werden. Ihre Stütze findet diese Hypothese in der geometrischen Anschauung, dass die Multiplikation einer reellen Grösse mit dem Koeffizienten $e^{\frac{\pi}{n}\sqrt{-1}}$ oder $\sqrt[n]{-1}$ der Drehung eines Radius in der Grundebene um den Winkel $\frac{\pi}{n}$ entspricht, dass aber im Raume von Haus aus keine Ebene als Grundebene gegeben ist, man also jede Ebene (sowohl jede durch eine bestimmte Axe gehende, als auch jede andere Ebene im Raume) zur Grundebene nehmen kann.

Die sehr begreifliche Thatsache, dass der konkrete Raum keine in der Abstraktion bestehende feste Grundebene haben kann, gleichwie er auch keine feste Einheit, keinen festen Nullpunkt und keine feste Grundaxe besitzt, dass man vielmehr die abstrakten arithmetischen Vorstellungen auf jede beliebige Anfangsstelle, Einheit, Grundaxe, Grundebene übertragen kann, hat zu einer grossen Täuschung Veranlassung gegeben: die Nichtexistenz absoluter Einheiten im konkreten, anschaulichen Raume, oder das Nichtgegebensein fester Einheiten ist mit Variabilität derselben verwechselt worden. Wir können jede Länge zur Längeneinheit, jeden Punkt im Raume zum Nullpunkte, jede durch diesen Punkt gehende Linie zur Grundaxe, jede durch diese Axe gehende Ebene zur Grundebene annehmen: ist Das aber geschehen; so können wir im Laufe der Rechnung diese Grundlagen nicht willkürlich ändern, sondern müssen sie unbedingt fest halten. Jede andere Länge, jeder andere Punkt, jede andere Axe, jede andere Ebene muss dann zu jenen festen Grundlagen in eine ganz bestimmte gesetzliche Beziehung treten, und jeder Fortschritt in irgend einer bestimmten Richtung, jede Drehung um eine bestimmte Axe muss zu dem primären Fortschritte längs der Grundaxe und zu der primären Drehung in der Grundebene eine ganz bestimmte gesetzliche Beziehung annehmen oder eine bestimmte Funktion davon sein.

Eine zweite Täuschung hat die Vieldeutigkeit der Wurzelgrössen hervorgerufen. Dieselbe beruht durchaus nicht auf einer Unbestimmtheit des Radikationsprozesses, auch nicht auf einer absoluten Unbestimmbarkeit des Radikands, sondern lediglich auf der thatsächlichen Nichtbestimmung oder unvollständigen Bestimmung des Radikands. Nur indem man es unterlässt, zu bestimmen, ob die Grösse 1 das Resultat keiner Umdrehung, also $= e^{0i}$, oder das Resultat einer ganzen Umdrehung, also $= e^{2\pi i}$, oder das Resultat zweier ganzen Umdrehungen, also $= e^{4\pi i}$ u. s. w. ist, nimmt $\sqrt[n]{1} = e^{\frac{2r\pi}{n}i}$ n verschiedene Werthe an: bestimmt man den Radikand 1 vollständig; so ist von keiner Unbestimmtheit der n-ten Wurzel die Rede; der Radikationsprozess ist nicht im mindesten unbestimmt, und eine vollständig gegebene Grösse ist es auch nicht.

Auch ohne diese spezielle Erläuterung ist es sonnenklar, dass, wenn die zweite Wurzel aus -1 einmal den Werth i und ein anderes Mal einen anderen Werth j ergeben soll, bei dieser zweiten Operation entweder der Wurzelausziehungsprozess ein anderer sein muss, oder der Radikand

— 1 einen anderen Werth haben muss: aus identisch derselben Grösse durch identisch denselben Prozess ein vom ersten abweichendes Resultat zu gewinnen, ist eine offenbare logische Absurdität. Mag nun die Verschiedenheit im Radikationsprozesse, oder mag sie im Werthe des Radikands liegen; immer muss sie erkennbar, definirbar, durch Funktionen darstellbar sein, wenn sich die Grössen und Prozesse in ein mathematisch gesetzliches System einreihen oder arithmetisch miteinander verknüpfen lassen sollen. Solange Diess nicht geschieht, sind die Ausdrücke Haupteinheiten für verschiedene Werthe i_1, i_2, i_3, welche die Grösse $\sqrt{-1}$ anzunehmen fähig sein soll, hohle Namen ohne Sinn, die Formeln wie $\sqrt{-1} = i_1$, $\sqrt{-1} = i_2$, $\sqrt{-1} = i_3$ oder $(i_1)^2 = -1$, $(i_2)^2 = -1$, $(i_3)^2 = -1$, $i_1 i_2 = i_3$ Absurditäten, die daraus gezogenen Schlüsse $(i_1)^2 - (i_2)^2 = 0$ ganz falsch, die daraus gebildeten Funktionen wie die Quaternionen $a + b i_1 + c i_2 + d i_3$ Kompilationen unverstehbarer Symbole und die Rechnungen mit solchen Phantasmen der Quell fortgesetzter Irrthümer.

Die Haupteinheiten i_1, i_2, i_3 sind nichts Anderes als Zeichen für ganz heterogene Objekte, die in keinem angebbaren Zusammenhange stehen. Man kann mit heterogenen Dingen gewisse mathematische Operationen vornehmen, man kann jedes Ding für sich vergrössern und verkleinern, kann dasselbe in seinem Gebiete verschieben und drehen, kann diese Dinge zugleich betrachten, kann ihnen gleichartige und ungleichartige Dinge hinzufügen und solche Dinge von ihnen hinwegnehmen, also im Sinne der Kompilation und der Beseitigung heterogene Grössen addiren und subtrahiren, man kann die Entstehung des einen Objektes in seinem Gebiete zu einer Regel für die Veränderung eines heterogenen Objektes in dessen Gebiete nehmen und in diesem Sinne heterogene Objekte miteinander multipliziren; man kann aber niemals ein Objekt mit einem heterogenen Objekte nach solchen Regeln verbinden, welche die gesetzlichen Veränderungen der Grössen einunddesselben Gebietes oder die Zugehörigkeit zu einunddemselben Gebiete oder die Homogenität der Objekte zur wesentlichen Voraussetzung haben. Hierzu gehört unter Anderem die Aneinanderreihung der Objekte mit ihren Anfängen und Enden, also die eigentliche Addition, sowie die Resultantenbildung aus mehreren gleichartigen Gliedern oder die Herstellung eines Vektors, welcher von dem allgemeinen Nullpunkte nach dem Endpunkte mehrerer aneinandergereiheten Grössen führt, und welcher bei homogenen Grössen der Formel $a + b i = r e^{\varphi i}$ entspricht.

So kann man z. B. 3 Zahleneinheiten, 2 Pfund, 5 Stunden und 4 Gedichte zusammen betrachten und dieses Agglomerat A durch die Formel

$$A = 3 + 2 i_1 + 5 i_2 + 4 i_3$$

ausdrücken, worin das Zeichen + ein Zusammensein oder eine Vereinigung im Sinne der Numeration, nicht eine Anreihung im Sinne der Addition bedeutet; denn offenbar haben Zahlen, Pfunde, Stunden und Gedichte keine gemeinsamen Endpunkte, an welchen sie sich verknüpfen liessen. Ebenso wenig kann man diesem Agglomerate den Werth einer einfachen Resultante oder eines Vektors von der Form $r e^{\varphi i}$ zuschreiben, welcher den

Werth jenes Agglomerates in einem Gebiete gleichartiger Grössen darstellt; denn es giebt für Zahlen, Pfunde, Stunden und Gedichte keine gemeinsame Qualität oder Dimensität, welche sie als gleichartige Grössen eines bestimmten Gebietes erscheinen lassen könnte.

Wenn man die Quaternion als ein Haufwerk heterogener Grössen, die Zeichen + und — zwischen diesen Grössen als Operationszeichen für die Zusammenhäufung und Ausscheidung (Numeration und Denumeration) und die Multiplikation wie eine Multiplikation heterogener oder verschieden dimensionirter Objekte ansieht, sodass in dem Produkte $a i_1 \times b i_2 = a b \,.\, i_1 i_2$ der Faktor $a b$ die Menge der Einheiten darstellt, welche die resultirende Grösse $a b\, i_1 i_2$ in einem Gebiete besitzen würde, das die fingirte und neue Qualität $i_1 i_2$ hat; so kann man die gewöhnlichen Additions- und Multiplikationsregeln darauf anwenden, also z. B. aus den Gleichungen

$$A = a + a_1 i_1 + a_2 i_2 + a_3 i_3$$
$$B = b + b_1 i_1 + b_2 i_2 + b_3 i_3$$

durch Addition das Resultat

$$A + B = (a + b) + (a_1 + b_1) i_1 + (a_2 + b_2) i_2 + (a_3 + b_3) i_3$$

sowie durch Multiplikation das Resultat

$$\begin{aligned} AB = {} & a b + a_1 b_1 i_1^2 + a_2 b_2 i_2^2 + a_3 b_3 i_3^2 \\ & + (a b_1 + a_1 b) i_1 + (a b_2 + a_2 b) i_2 + (a b_3 + a_3 b) i_3 \\ & + (a_1 b_2 + b_1 a_2) i_1 i_2 + (a_1 b_3 + a_3 b_1) i_1 i_3 + (a_2 b_3 + a_3 b_2) i_2 i_3 \end{aligned}$$

ziehen, (was wir auch in den obigen Rechnungen mit dreidimensionalen Grössen in §. 17 Nr. 2 bis 5 gethan haben): allein, es ist durchaus unzulässig, die Glieder von verschiedenen Dimensitäten oder Qualitäten, also die in $1, i_1, i_2, i_3, i_1^2, i_2^2, i_3^2, i_1 i_2, i_1 i_3, i_2 i_3$ multiplizirten Glieder nach den für gleichartige Grössen geltenden Regeln zu vereinigen. Sowie Diess geschieht, stellen sich sofort die grössten Ungereimtheiten ein. Wie geht es nun zu, dass dessenungeachtet der Quaternionenkalkul Resultate liefert, welche mit den Resultaten der konstruirenden Geometrie übereinstimmen? Das wird hervorgebracht durch allerlei spezielle Einschränkungen der Rechnung, durch Aufhebung gewisser sonst allgemeingültiger Sätze (z. B. über die Vertauschbarkeit der Faktoren eines Produktes) und durch willkürliche, den allgemeinen Prinzipien widersprechende Ausdeutung der Operationen (z. B. dadurch, dass die Multiplikation mit gewissen Faktoren, welche sonst nur Vervielfältigung und Drehung bedeutet, nun Verschiebung, also eine Wirkung bedeuten soll, welche prinzipiell der Addition zukömmt), durch gelegentliche Umdeutung einunderselben Grösse (z. B. dadurch, dass eine Grösse j_α bald ein Drehfaktor um den Winkel α, bald ein Verschiebungsfaktor um die Länge und in der Richtung des Vektors α sein soll), durch stumme Überspringung klaffender Lücken (z. B. der Frage, wenn der Verschiebungsfaktor j das erste Glied des Polynoms $a + b + c$ oder die erste Seite des Polygons $a + b + c$ vermöge der Formel $ja + b + c$ verschiebt, welche Macht denn die folgenden Glieder b und c verschiebt, ob dieselben, stehen bleibend, sich vom ersten Gliede trennen, oder ob sie ohne Verschiebungsfaktor mitrücken und in letzterem Falle, wie sich denn der Ausdruck $ja + b + c$

von dem Ausdrucke $ja + jb + jc$ unterscheidet). Diese Einschränkungen, Ausnahmen und Ausdeutungen bilden eine fortgesetzte Korrektur und Einrenkung, welcher die allgemeinen Formeln lediglich durch den Hinblick auf die geometrischen Effekte, welche sie hervorbringen sollen, unterzogen werden. Der Quaternionenkalkul ist keine strenge arithmetische Rechnung, sondern ein Gemisch von Rechnung und geometrischer Konstruktion, ein Verfahren, welches im Interesse dieser Konstruktion seinen Standpunkt wählt und ändert, indem es gewisse Theile der Operation auf diese, gewisse andere Theile auf jene geometrischen Verhältnisse bezieht, also in ähnlicher Weise zu Werke geht, wie die sogenannte analytische Geometrie, die auch theils rechnet, theils konstruirt und gewisse reelle Grössen in dieser Richtung, gewisse andere reellen Grössen in jener Richtung mischt, gewisse reelle Grössen für gerade Linien, gewisse andere reellen Grössen für Kreisbögen oder für Winkel oder für Flächen oder für Körper erklärt, ohne sich um die arithmetische Beziehung dieser Grössen auf Grund der Bedeutung des Imaginären, des Richtungskoeffizienten, der Dimensität, der Homogenität und Heterogenität und aller anderen Grundeigenschaften und Grundgesetze, durch welche sich ein abstraktes Grössensystem auferbauet, zu kümmern.

Unser Situationskalkul ist von ganz anderer Art: er zeigt die Übereinstimmung des arithmetischen Begriffes mit der räumlichen Anschauung, aber er begründet nicht das allgemeinere arithmetische Gesetz durch das speziellere geometrische. Mit unseren triplexen und polydimensionalen Grössen kann man nach allgemeinen Regeln rechnen und gewiss sein, dass das Resultat mit Nothwendigkeit einem geometrischen Gesetze entspricht, ohne dass diese Übereinstimmung durch besondere Einschränkungen und Ausnahmen von allgemeinen Regeln gesichert zu werden braucht.

Es ist leicht zu erkennen, dass die Hamiltonsche Quaternion der falschen Entwicklung einer Verhältnisszahl $e^{\varphi i}\, e^{\psi i_1}$ in ein Polynom nach der Formel

$$\begin{aligned} e^{\varphi i}\, e^{\psi i_1} &= \cos\varphi\, \cos\psi + \cos\varphi\, \sin\psi\, .\, i_1 \\ &\quad + \sin\varphi\, \cos\psi\, .\, i + \sin\varphi\, \sin\psi\, .\, i i_1 \end{aligned}$$

entspricht, während die richtige Entwicklung

$$e^{\varphi i}\, e^{\psi i_1} = \cos\varphi + \sin\varphi\, \cos\psi\, .\, i + \sin\varphi\, \sin\psi\, .\, i i_1$$

erfordert, und dass in der Theorie der Quaternionen die in §. 17 Nr. 6 erörterte Verschiedenheit des Begriffes der Gleichheit, jenachdem man den Standpunkt im Fortschritts-, oder im Verhältnissgesetze nimmt, nicht beachtet ist.

Hiernach vermag ich auch nicht den Ansichten beizustimmen, welche Dedekind in einer Abhandlung über die aus n Haupteinheiten gebildeten Grössen in den Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen vom 23. März 1885 ausspricht, soweit sie die Bedeutung dieser Grössen und ihre Einreihung unter die algebraischen Zahlen betreffen. Meines Erachtens sind die algebraischen Zahlen, wie schon in vorhergehender Nummer erwähnt ist, Gebilde in der zweidimensionalen Ebene, und die aus Haupteinheiten gebildeten Grössen sind, wenn sie nicht auf die einzige Haupteinheit $i = \sqrt{-1}$ eingeschränkt werden, sondern in

den dreidimensionalen Zahlenraum eintreten sollen, nur mit Hülfe eines ganz neuen Operationszeichens cominus ($\div$) zu begründen und nicht nach den Rechnungsregeln, welche für die gewöhnlichen komplexen Grössen gelten, zu behandeln.

VI. Die Kugeltheilung.

§. 21. Die regelmässige Eintheilung der Kugeloberfläche.

1) In §. 17 haben wir gezeigt, dass die Gleichung p-ten Grades p^2 triplexe Wurzeln hat. Durch Division mit $x - 1$ wird die Gleichung $x^p - 1$ von allen denjenigen Wurzeln befreiet, welche der Einheit 1 gleich sind oder dieselbe geometrisch decken, also von den p Wurzeln $e^{0 i_1}$, $e^{\frac{2\pi}{p} i_1}$, $e^{\frac{4\pi}{p} i_2}$, ... Die Gleichung $x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$, worin p eine Primzahl sei, enthält also noch $(p-1)^2$ triplexe Wurzeln, welche der allgemeinen Form $x = e^{\frac{2r\pi}{p} i} \; e^{\frac{2s\pi}{p} i_1}$ entsprechen, wenn man darin r und s zwischen den Zahlen 1, 2, 3, ... $p - 1$ variiren lässt. Schreibt man $x = e^{\frac{2\pi}{p}(ri + si_1)}$; so leuchtet ein, dass man für den Exponenten $ri + si_1$ (worin das Zeichen $+$ nicht als Additions-, sondern lediglich als Akkumulations- oder Numerationszeichen zu betrachten ist) auch die kleinsten positiven Reste der Funktion $a^m i + a^n i_1$ nach dem Model p nehmen kann, worin a eine primitive Wurzel der Kongruenz $x^{p-1} - 1 \quad 0 \; mod \; p$ bedeutet und die beiden Exponenten m und n unabhängig voneinander die Reihe von $p - 1$ aufeinander folgenden ganzen Zahlen durchlaufen, sodass also für jeden Werth von m aus der Reihe 0, 1, 2, ... $p - 2$ der Exponent n dieselbe Reihe 0, 1, 2, ... $p - 2$ durchläuft. Für jedes bestimmte m erhält man also eine Grundtafel von $p - 1$ Resten; jede dieser Partialtafeln zerfällt wie die für komplexe Wurzeln einer Gleichung $(p-1)$-ten Grades aufgestellte Grundtafel in Perioden, kann also wie diese behandelt werden, wodurch die Bestimmung ihrer einzelnen Elemente auf die Auflösung von Gleichungen, deren Grade Faktoren von $p - 1$ sind, zurückgeführt wird.

Aus §. 17 Nr. 4 geht übrigens hervor, dass man die Zerlegung der allgemeinen Grundtafel in $p - 1$ Partialtafeln unter zwei verschiedenen Gesichtspunkten bewirken kann: einmal für eine konstante, allen Elementen gleiche Inklination, d. h. für einen konstanten Werth von n, und einmal für eine gleichmässige Variation der Inklination und Deklination der Elemente, also für eine gleiche Zunahme der Exponenten m und n.

Da die Reste von a^m keine anderen sind, als die von a^n, sondern nur eine andere Reihenfolge beobachten können; so lassen sich die Partialtafeln aus der früheren Grundtafel für komplexe Wurzeln leicht zusammenstellen. Wir übergehen Diess und beschränken uns auf eine Bemerkung über die geometrische Bedeutung der vorliegenden Zahlengesetze.

Theilt man einen in der Grundebene XYZ des Raumes um den Nullpunkt O beschriebenen Kreis vom Radius 1 in p gleiche Theile und

zieht nach den Theilpunkten die p Radien; so entsprechen die Richtungen derselben den durch Drehung des Grundradius entstehenden Deklinationskoeffizienten e^{0i}, $e^{\frac{2\pi}{p}i}$, $e^{\frac{4\pi}{p}i}$ u. s. w. Wälzt man die so eingetheilte Grundebene um die Grundaxe OX, oder theilt man einen in der tertiären Ebene YOZ um den Nullpunkt beschriebenen Kreis vom Radius 1 in p gleiche Theile und legt durch die Theillinien und die Grundaxe die p Meridianebenen mit ihren deklinirenden Radien; so entsprechen die Richtungen dieser Meridianebenen den Inklinationskoeffizienten e^{0i_1}, $e^{\frac{2\pi}{p}i_1}$, $e^{\frac{4\pi}{p}i_1}$, irgend ein Radius in irgend einer Meridianebene repräsentirt also den Richtungskoeffizienten $e^{\frac{2r\pi}{p}i}\ e^{\frac{2s\pi}{p}i_1}$.

Die Operation mit konstanter Inklination ist ein Prozess in einer einzelnen Meridianebene. Die Operation mit gleichmässiger Variation der Inklination und Deklination ist ein die verschiedenen Meridianebenen mit veränderlicher Richtung durchspringender Prozess.

Durch die Gesammtheit der p verschiedenen Radien in den p verschiedenen Meridianen wird der dreidimensionale Raum oder die Kugel in regelmässiger Weise nach Meridianen und nach Parallelkreisen abgetheilt. Verbindet man den Endpunkt jedes Radius mit den ihm in demselben Meridiane und Parallelkreise zunächst liegenden Endpunkten, also mit den vier nächsten Punkten (welche sich nur für einen Polpunkt auf drei Punkte reduziren), durch gerade Linien; so stellt sich ein Netzwerk von viereckigen Maschen dar. Die beiden in Parallelkreisen liegenden Seiten einer Masche sind parallel und die beiden in Meridianebenen liegenden Seiten konvergiren nach einem Punkte der Grundaxe. Jede Masche bildet daher ein ebenes Paralleltrapez, durch welches sich eine Ebene legen lässt. Alle diese Ebenen bilden ein Polyeder von p^2 Trapezflächen, dessen Ecken sämmtlich in der Oberfläche einer Kugel vom Radius 1 liegen, und von welchem alle zwischen zwei Parallelkreisen liegenden Flächen einander kongruent sind und gleiche Neigung gegeneinander haben. Dieses Polyeder entsteht durch die Umwälzung eines ebenen Polygons von p Seiten um die Grundaxe.

Diese Kugeltheilung ist von dem Werthe der Zahl p unabhängig, sie findet so gut für prime, wie für zusammengesetzte Werthe von p statt. In dem Pole, für welchen der Richtungskoeffizient gleich $e^{0i}\ e^{0i_1}$ ist, und welchen wir den positiven Pol nennen, bildet sich immer eine wirkliche Ecke. Ist p eine paare Zahl; so bildet sich auch im negativen Pole eine solche Ecke, und man erhält das Bild, welches der Erdglobus darbietet, wenn man alle Schnittpunkte der Parallel- und Meridiankreise miteinander verbindet. Ist aber p unpaar; so entsteht im negativen Pole keine Ecke, sondern in jedem meridionalen Ausschnitte eine ebene trapezförmige Fläche, deren schräge Seiten sich im Pole kreuzen. Für die verschiedenen meridionalen Ausschnitte verschieben sich diese Figuren im Kreise neben- und übereinander und bilden in ihrer Gesammtheit ein ebenes regelmässiges sternförmiges Polygon von $2p$ Seiten, und das ganze Polyeder stellt sich als ein sternförmiges Polyeder von p^2 einander durchdringenden Seitenflächen dar, worin der positive Pol eine aus zwei gegeneinander verdrehten Pyramiden bestehende Doppelspitze bildet.

Wenn man in diesem Polyeder anstatt von dem einen Punkte zum nächsten zu schreiten, immer einen oder zwei oder n Punkte überspringt, also $e^{\frac{2n\pi}{p}i}$ und $e^{\frac{2n\pi}{p}i_1}$ resp. an die Stelle von $e^{\frac{2\pi}{p}i}$ und $e^{\frac{2\pi}{p}i_1}$ setzt, verwandelt man das sich umwälzende Grundpolygon in ein Sternpolygon mit mehrmaliger Umdrehung, sowie die Wälzung in eine mehrmalige Umwälzung. Hierdurch entsteht ein sternförmiges Polyeder mit p^2 sich mehrfach durchschneidenden Seitenflächen.

2) Die Arithmetik, als abstrakte Mathematik, verlangt Absolutheit oder unbedingte Festigkeit der Basen der Grundoperationen: die Multiplikation kann nur eine Verhältnissbildung aus einer festen Einheit sein, oder muss sich stets auf dieselbe Einheit beziehen. Demnach ist primäre Multiplikation die Bildung eines Quantitätsverhältnisses (resp. Vervielfältigung) aus einer festen Quantitätseinheit 1: durch fortgesetzte primäre Multiplikation entstehen alle reinen Grössenverhältnisse oder die absolute Zahlenreihe oder die Grundreihe. Sekundäre Multiplikation ist die Bildung eines Neigungsverhältnisses jeder Quantität oder des ganzen Gebietes aller Quantitäten gegen die Richtung der absoluten Zahlenreihe, also gegen eine feste Grundrichtung, welche mit dem Koeffizienten $+1$ oder $(-1)^0$ oder e^{0i} bezeichnet wird, sodass die sekundäre Multiplikation eine Multiplikation mit dem Deklinationskoeffizienten $(-1)^\alpha = e^{\alpha i}$ ist und immer eine Abweichung von der festen Grundrichtung $+1$ darstellt: durch fortgesetzte primäre und sekundäre Multiplikation entsteht die komplexe Zahlenebene oder die Grundebene. Tertiäre Multiplikation ist die Bildung eines Neigungsverhältnisses jeder deklinanten Grösse oder des ganzen Gebietes aller deklinanten Quantitäten gegen die feste Grundebene, deren Richtung mit dem Koeffizienten $\dot{+}1$ oder $(\dot{+}1)^0$ oder e^{0i_1} bezeichnet wird, sodass die tertiäre Multiplikation eine Multiplikation mit dem Inklinationskoeffizienten $(\dot{+}1)^\beta = e^{\beta i_1}$ ist und immer eine Abweichung von der festen Grundebene darstellt: durch fortgesetzte primäre, sekundäre und tertiäre Multiplikation entsteht der triplexe oder dreidimensionale Zahlenraum. Der in voriger Nummer betrachtete Prozess entspricht der regelmässigen Raumtheilung in arithmetischem Sinne, indem danach die Deklination gegen die Grundaxe und die Inklination gegen die Grundebene in gleichen Absätzen variirt: das dort beschriebene Polyeder ist ein absolut regelmässiger Körper nach arithmetischer Auffassung, welche den Standpunkt der Betrachtung bei dem Verlaufe des Bildungsprozesses fortwährend in der festen Einheit, in dem festen Nullpunkte, in der festen Grundaxe und in der festen Grundebene beibehält.

Die Geometrie, als anschauliche Mathematik oder als Erkenntniss des Raumes, welcher ein äusseres Objekt, ein Anschauungsobjekt ist, kennt keine absoluten oder festen Basen. Der erkennende Geist trägt bei der Erkenntniss der Aussenwelt seine eigenen Basen, welche für ihn die absolut festen sind, in diese Welt hinein, um die äusseren Grössenverhältnisse darauf zu beziehen. Wir können jede Länge zur Einheit, jeden Punkt im Raume zum Nullpunkte, jede durch diesen Punkt gehende Linie zur Grundaxe, jede durch diese Axe gehende Ebene zur Grundebene annehmen. Nachdem Diess geschehen, entsprechen gewisse

geometrische Prozesse den eben erwähnten arithmetischen, die verhältnissmässige Ausdehnung der quantitativen Verhältnissbildung, die Drehung um den Nullpunkt in der Grundebene oder gegen die Grundaxe (bei der Inklination null) der Deklination, die Wälzung um die Grundaxe der Inklination. Man kann sagen, der Raum, wie jedes Auschauungsgebiet habe, dem Erkenntnissvermögen gegenüber, keine absoluten, sondern relative Basen. Dieser relative Standpunkt des Raumes, welcher sein naturgemässer ist, da er thatsächlich ohne feste Basen gegeben oder dem reinen Verstande zur Erkenntniss, d. h. zur Anpassung an dessen festes System dargeboten ist, verleihet den rein geometrischen Prozessen, Konstruktionen und sonstigen Anschauungen etwas Eigenartiges, welches zwar sein arithmetisches Korrelat hat, aber doch von diesem Korrelate nicht in allen Nebeneigenschaften, namentlich nicht in dem Wege der leichtesten Darstellbarkeit und Anschaulichkeit gedeckt wird. Die Verschiedenheit der Mittel, deren sich die reine Abstraktion oder Rechnung und die geometrische Konstruktion bedient, bedingen bald auf der einen, bald auf der anderen Seite eine grössere Schwierigkeit und Komplikation. So lassen sich z. B. die Durchschnitte von Kurven oftmals leicht konstruiren, aber schwer berechnen, manche auf jener Konstruktion beruhenden Konfigurationen oft leicht übersehen, aber schwierig in Formeln darstellen.

Zu den Eigenartigkeiten der Raumanschauung gehört auch die Leichtigkeit des Wechsels des Standpunktes der Betrachtung. Unter Zulassung eines solchen Wechsels gewinnt die geometrische Regelmässigkeit der Raumeintheilung eine besondere Bedeutung, wenn man bei der Anschauung der betreffenden Figur den Ausgangspunkt der Betrachtung oder die Basen des Raumes, also den Nullpunkt, die Grundaxe und die Grundebene fortgesetzt verlegt, indem man also die Figur nicht von einem einzigen Grundsysteme aus betrachtet und alle ihre Verhältnisse auf dieses einzige System bezieht, sondern indem man die Figur von jeder Ecke, als von einem Nullpunkte mit zugehörigem besonderen Grundsysteme, aus betrachtet. Geometrisch regelmässig erscheint alsdann die Figur, wenn die Verhältnisse, welche sie von den verschiedenen Nullpunkten, bezw. Grundsystemen aus darbietet, sich sämmtlich gleich sind, also wenn sie für verschiedene Ausgangspunkte gleiche relative Verhältnisse hat.

Für das zweidimensionale oder komplexe Grössengebiet fällt arithmetische und geometrische Regelmässigkeit der Figur zusammen; für das dreidimensionale oder triplexe und jedes höher dimensionirte Gebiet jedoch nicht. Das vorhin betrachtete arithmetisch regelmässige Polyeder hat keine geometrische Regelmässigkeit, und ein geometrisch regelmässiges Polyeder, wie z. B. das Tetraeder, Hexaeder u. s. w. hat keine arithmetische Regelmässigkeit. Wegen des Zusammenfallens der arithmetischen und der geometrischen Regelmässigkeit im zweidimensionalen Gebiete giebt es sowohl arithmetisch, als auch geometrisch unendlich viel reguläre Polygone, wogegen es bei der Verschiedenheit jener Prinzipien im dreidimensionalen Gebiete wohl unendlich viel arithmetisch regelmässige, aber nur wenige geometrisch regelmässige Polyeder giebt.

Soviel liegt auf der Hand, dass die arithmetischen Rechnungsregeln, welche sich auf feste Basen stützen, nicht ohne Weiteres auf Operationen

anwendbar sind, bei welchen der Wechsel der Basen zum Prinzip erhoben wird. Demzufolge ist es undenkbar und widersinnig, die Multiplikation mit dem Deklinationskoeffizienten $e^{\alpha i}$, welche eine Drehung gegen eine feste Grundaxe OX bedeutet, oder die Multiplikation mit dem Inklinationskoeffizienten $e^{\beta i_1}$, welche eine Wälzung um diese feste Grundaxe anzeigt, als eine Drehung gegen jede beliebige Linie, bezw. als eine Wälzung um eine beliebige Linie anzusehen, oder überhaupt Drehungen und Wälzungen um variabele Linien oder für variabele Basen wie absolute arithmetische Prozesse zu behandeln oder mit festen Formeln zu belegen, wie es in neuerer Zeit verschiedentlich, namentlich auch im Quaternionenkalkul erfolglos und zum Schaden einer rationellen wissenschaftlichen Behandlung der Sache versucht ist.

Dem geometrischen Wechsel des Standpunktes entspricht zunächst ein Wechsel der Basen. Wenn Letzterer in den Formeln gehörigen Ausdruck gefunden hat, können die auf die neuen Basen bezüglichen Drehungen und Wälzungen an diesen Formeln nach den allgemeinen arithmetischen Regeln vollzogen werden.

3) Um nach dieser einfachen Regel die Formeln für einen regelmässigen Körper abzuleiten, sei der Mittelpunkt O einer mit dem Radius 1 beschriebenen Kugel der Nullpunkt, $ABCDE$ in Fig. 17 eine Seitenfläche des Körpers, welche ein regelmässiges Polygon von m Seiten bilde, M der Mittelpunkt dieses Polygons, OM die reelle Grundaxe, MOA die Grundebene der komplexen Zahlen, sodass die tertiäre Axe OZ senkrecht auf dieser Ebene steht. Bezeichnet α den Winkel AOM; so ist die Linie $OA = e^{\alpha i} = \cos\alpha + \sin\alpha \,.\, i$. Ist $\beta = \frac{2\pi}{m}$ der Winkel BMA oder der Neigungswinkel der Ebene BOM gegen die Ebene AOM; so ist die Linie $OB = e^{\alpha i}\, e^{\beta i_1}$, die Linie $OC = e^{\alpha i}\, e^{2\beta i_1}$, die Linie $OD = e^{\alpha i}\, e^{3\beta i_1}$ und die nach dem letzten Punkte E des Polygons $ABCDE$ führende Linie $OE = e^{\alpha i}\, e^{(m-1)\beta i_1} = e^{\alpha i}\, e^{-\beta i_1}$; man hat also nach dem Situationskalkul

$$OB = \cos\alpha + \sin\alpha\cos\beta \,.\, i + \sin\alpha\sin\beta \,.\, i\, i_1$$
$$OE = \cos\alpha + \sin\alpha\cos\beta \,.\, i - \sin\alpha\sin\beta \,.\, i\, i_1$$

Verlegt man jetzt die Grundaxe aus der Richtung OM in der Grundebene in die Richtung OA; so entspricht Diess einer Multiplikation des primären und sekundären Gliedes der auf die Grundaxe OM bezogenen Ausdrücke mit dem Richtungskoeffizienten $e^{-\alpha i} = \cos\alpha - \sin\alpha \,.\, i$.

In dem neuen Basensysteme hat man also

$$OB = (\cos^2\alpha - \sin^2\alpha\cos\beta) - \sin\alpha\cos\alpha(1 - \cos\beta)\, i + \sin\alpha\sin\beta \,.\, i\, i_1$$
$$OE = (\cos^2\alpha - \sin^2\alpha\cos\beta) - \sin\alpha\cos\alpha(1 - \cos\beta)\, i - \sin\alpha\sin\beta \,.\, i\, i_1$$

Der Inklinationskoeffizient einer Grösse $x + yi + zii_1$ ist $e^{\psi i_1} = \frac{y + z i_1}{\sqrt{y^2+z^2}}$. Bezeichnet man also die Inklination von OB mit ψ_1 und die von OE mit ψ_2; so ist die Inklination von OB gegen OE, d. h. der Neigungswinkel der Ebene EOA gegen BOA gleich $\psi_2 - \psi_1$, und wenn man denselben mit γ bezeichnet, ist

$$\frac{e^{\psi_2 i_1}}{e^{\psi_1 i_1}} = e^{(\psi_2 - \psi_1) i_1} = \sqrt{\frac{y_1^2 + z_1^2}{y_2^2 + z_2^2}} \cdot \frac{y_2 + z_2 i_1}{y_1 + z_1 i_1}$$

Eine Substitution aus den Werthen von OB und OE giebt

$$e^{\gamma i_1} = \frac{\cos\alpha\,(1 - \cos\beta) + \sin\beta\, i_1}{\cos\alpha\,(1 - \cos\beta) - \sin\beta\, i_1}$$

und wenn man Zähler und Nenner mit $\cos\alpha\,(1 - \cos\beta) + \sin\beta\, i_1$ multiplizirt (indem man zuvor i an die Stelle von i_1 setzt, um nach Vollendung der Rechnung die Vertauschung wieder zu redressiren),

$$\cos\gamma = \frac{\cos^2\alpha\,(1 - \cos\beta)^2 - \sin^2\beta}{\cos^2\alpha\,(1 - \cos\beta)^2 + \sin^2\beta}$$

$$\sin\gamma = -\frac{2\cos\alpha\,\sin\beta\,(1 - \cos\beta)}{\cos^2\alpha\,(1 - \cos\beta)^2 + \sin^2\beta}$$

Aus der ersten dieser beiden Gleichungen folgt

$$\cos\alpha = \frac{\sin\beta}{1 - \cos\beta}\sqrt{\frac{1 + \cos\gamma}{1 - \cos\gamma}} = \cot\frac{\beta}{2} \cdot \cot\frac{\gamma}{2} = \cot\frac{\pi}{m} \cdot \cot\frac{\pi}{n}$$

Es liegt auf der Hand, dass, wenn $\gamma = \frac{2\pi}{n}$ ist, die Linie OB durch n-malige Wälzung um den Winkel γ um die Linie OA nachundnach die Lagen der Kanten OB, OE, OF einer n-seitigen regelmässigen Pyramide durchläuft, oder dass sich das Polygon, welches die eine Seitenfläche $ABCDE$ bildet, n-mal aneinander lagert, um eine n-seitige Ecke um den Punkt A zu bilden. Ganz das Nämliche wird sich in jeder Ecke der ursprünglichen und jeder später erzeugten Seitenfläche ereignen, und daraus geht hervor, dass sich nothwendig die ganze Kugel mit gleichen regelmässigen Polygonen unter gleichen Neigungen vollständig bedecken wird. Die vorstehende Gleichung für $\cos\alpha$ ist die einzige Bedingung für jeden möglichen regelmässigen Körper. Zu ihrer Erfüllung ist nur nöthig, dass der Werth von $\cot\frac{\pi}{m} \cdot \cot\frac{\pi}{n}$ kleiner als 1 ausfalle, alle Werthe von m und n, welche diese Bedingung erfüllen, liefern einen regelmässigen Körper, sonst keine. Dass die Werthe 1 und 2 für m oder n, sowie die Werthe 0 und 1 für $\cot\frac{\pi}{m} \cdot \cot\frac{\pi}{n}$ ausgeschlossen sind, leuchtet ein. Zur Prüfung der möglichen Fälle hat man also $m = 3, 4, 5 \ldots$ und $n = 3, 4, 5 \ldots$ zu untersuchen. Es findet sich leicht, dass nur für

$m =$	3	3	3	4	5
$n =$	3	4	5	3	3

$\cot\frac{\pi}{m} \cdot \cot\frac{\pi}{n} < 1$ wird, dass es also nur fünf regelmässige Körper giebt, nämlich drei Körper mit dreieckigen Seitenflächen und resp. drei-, vier- und fünfkantigen Ecken, nämlich das Tetraeder, das Oktaeder und das Ikosaeder, ferner einen Körper mit viereckigen Seitenflächen und drei-

kantigen Ecken, nämlich das Hexaeder, und einen Körper mit fünfeckigen Seitenflächen und dreikantigen Ecken, nämlich das Dodekaeder.

Die Formel für $\cos \alpha$ lehrt, dass die Winkel β und γ oder die Zahlen m und n unbeschadet des Werthes von α vertauschbar sind, dass also, wenn es einen regelmässigen Körper mit m-eckigen Seitenflächen und n-kantigen Ecken giebt, es auch stets einen Körper mit n-eckigen Seitenflächen und m-kantigen Ecken giebt, und dass für beide der Winkel $AOM = \alpha$ gleich gross ist. Demzufolge hat dieser Winkel für das Oktaeder und das Hexaeder, ferner für das Ikosaeder und für das Dodekaeder gleichen Werth.

Ob die vorstehende Formel für $\cos \alpha$ schon bekannt ist, weiss ich nicht; übrigens glaube ich, dass eine einfachere Ableitung derselben, ohne alle geometrische Hülfskonstruktion, kaum denkbar ist, dass also auch dieses Beispiel die Kraft des Situationskalkuls in ein helles Licht setzt.

Ich bemerke noch, dass jene Formel sofort alle wesentlichen Stücke eines regelmässigen Körpers in einfachen und zur logarithmischen Rechnung geschickten Formeln ergiebt. Wenn R der Radius OA der umschriebenen Kugel ist; so ist der Radius der eingeschriebenen Kugel $OA = R \cos \alpha = R \cot \frac{\pi}{m} . \cot \frac{\pi}{n}$, und der Radius des um eine Seitenfläche beschriebenen Kreises ist

$$MA = R \sin \alpha = \frac{R \sqrt{\cos\left(\frac{1}{m} - \frac{1}{n}\right)\pi . \cos\left(1 - \frac{1}{m} - \frac{1}{n}\right)\pi}}{\sin \frac{\pi}{m} \sin \frac{\pi}{n}}$$

also der Radius des in ein Seitenpolygon beschriebenen Kreises $MN = R \sin \alpha \cos \frac{\pi}{m}$ und die Länge einer Seitenlinie dieses Polygons $AB = 2 R \sin \alpha \sin \frac{\pi}{m}$.

4) Die vorstehende Regelmässigkeit verlangt nicht unbedingt, dass die Winkel β und γ aliquote Theile von 2π, sondern von irgend einem Vielfachen von 2π seien, dass man also $\beta = \frac{2p\pi}{m}$, $\gamma = \frac{2q\pi}{n}$ habe. Ist $p > 1$; so bildet die Seitenfläche $ABCDE$ ein Sternpolygon, und ist $q > 1$; so bildet die Ecke $ABFE$ des Polyeders eine Sternecke. Übrigens lässt sich jetzt, da eine Sternfigur keinen bestimmten Raum einschliesst, nicht behaupten, dass durch die Nebeneinanderlegung von Sternfiguren der ganze Kugelraum erschöpft werden müsse, dass also jeder Werth von α ein regelmässiges Sternpolyeder bedinge. Wir können den Gegenstand hier nicht weiter verfolgen, bemerken aber, dass, wenn man alle Kanten eines Dodekaeders verlängert, sich je fünf Kanten in einem Punkte treffen, und dass die entstehende Figur ein regelmässiges Sterndodekaeder ist, dessen Seitenflächen sternförmige Fünfecke sind. Während das gewöhnliche Dodekaeder 20 dreikantige Ecken mit 30 Kanten besitzt, hat das Sterndodekaeder 12 fünfkantige Ecken mit 30

Kanten. Es giebt also zwei Dodekaeder und demzufolge mindestens sechs regelmässige Körper.

5) Die eben betrachtete Regelmässigkeit der Kugeltheilung geht von dem Gesichtspunkte aus, dass das regelmässige Polyeder immer die nämliche Beziehung seiner Theile zu einer Grundaxe darbiete, gleichviel, durch welchen Mittelpunkt M einer Seitenfläche oder auch durch welche Ecke A des Polyeders man diese Axe legen möge. Zieht man vom Mittelpunkte O der Kugel entweder nach allen Mittelpunkten M der Seitenflächen, oder nach allen Ecken A die Radien; so bezeichnen dieselben eine regelmässige Eintheilung des Raumes, indem sie sich um jeden einzelnen dieser Radien in regelmässigen Figuren, welche die Kanten von Pyramiden bilden, gruppiren. Die von der Spitze O auslaufenden Kanten einer Pyramide mit polygonaler Basis bilden allerdings eine regelmässige Figur im Sinne der Rotation um die Axe der Pyramide, aber doch keine absolut einfache Figur, oder sie haben keine vollkommene Regelmässigkeit in der Hinsicht, dass jede Kante zu jeder anderen Kante dieselbe Beziehung hätte; die erste Kante bildet mit der zweiten Kante im Allgemeinen einen anderen Winkel, als mit der dritten Kante. Nur wenn die kleinste oder Grundpyramide dreikantig ist, d. h. wenn je drei unmittelbar benachbarte Radien gleiche Neigung gegeneinander haben, liegt eine vollkommen regelmässige Raumeintheilung vor (abgesehen von dem Falle einer zweikantigen Pyramide mit dem Winkel von 180^0 an der Spitze oder dem Falle, wo der Raum durch zwei entgegengesetzte Radien abgetheilt ist).

Wenn man die Bedingung für diese regelmässige Raumeintheilung formuliren will, hat man zunächst auszudrücken, dass die Fläche des gleichseitigen sphärischen Dreieckes, welches durch die Grundpyramide gebildet wird, derjenige aliquote Theil der Kugelfläche sei, welcher der Anzahl dieser Pyramiden entspricht. Offenbar bedingen n Radien, welche die regelmässige Raumeintheilung bilden, welche also n Endpunkte der fraglichen sphärischen Dreiecke geben, $2(n-2)$ solcher Dreiecke; es muss also, wenn F der Flächeninhalt eines dieser Dreiecke ist, $2(n-2)F = 4\pi R^2$ sein. Wenn α der Neigungswinkel zweier Seitenflächen einer dreikantigen Ecke, also $3\alpha - \pi$ der sphärische Exzess des gleichseitigen sphärischen Dreieckes, mithin $F = (3\alpha - \pi)R^2$ ist; so muss

$$\alpha = \frac{n}{n-2} \cdot \frac{\pi}{3} \text{ sein.}$$

Wenngleich diese Bedingung nothwendig erfüllt werden muss; so ist sie doch zur Erfüllung der Aufgabe nicht ausreichend: es muss vielmehr noch konstatirt werden, dass alle diejenigen gleichseitigen sphärischen Dreiecke, welche sich mit einer gemeinschaftlichen Spitze nebeneinander legen, den betreffenden Kugelabschnitt ganz ausfüllen, dass also die Sehnen ihrer dritten Seiten ein regelmässiges Polygon in dem Kreise bilden, der die Basis dieses Kugelabschnittes ist. Ist m die Anzahl der Seiten dieses Polygons; so muss $\alpha = \frac{2\pi}{m}$ sein.

Diese und die vorher gefundene Bedingung zusammen erfordern, dass $m = 6 - \frac{12}{n}$, mithin n ein Faktor von 12 sei. Die möglichen Werthe für n, $2(n-2)$, m und α sind also

$$
\begin{array}{rcccccc}
n & = & 3 & 4 & 6 & 12 \\
2\,(n-2) & = & 2 & 4 & 8 & 20 \\
m & = & 2 & 3 & 4 & 5 \\
u & = & \pi & \frac{2\pi}{3} & \frac{\pi}{3} & \frac{2\pi}{5}
\end{array}
$$

Der erste Fall entspricht der Zweitheilung des Raumes durch zwei entgegengesetzte Radien; die übrigen drei Fälle bestätigen sich in der That an den sechs regelmässigen Körpern und zwar am Tetraeder sowohl durch die nach den 4 Mittelpunkten der Seitenflächen führenden Radien OM, als auch durch die nach den 4 Ecken führenden Radien OA, am Hexaeder durch die nach den 6 Mittelpunkten der Seitenflächen führenden Radien OM, jedoch nicht durch die nach den 8 Ecken desselben führenden Radien OA, am Oktaeder durch die nach den 6 Ecken führenden Radien OA, jedoch nicht durch die nach den 8 Mittelpunkten der Seitenflächen führenden Radien OM, am gewöhnlichen Dodekaeder durch die nach den 12 Mittelpunkten der Seitenflächen führenden Radien OM, jedoch nicht durch die nach den 20 Ecken desselben führenden Radien, am Sterndodekaeder sowohl durch die nach den 12 Mittelpunkten der Seitenflächen führenden Radien OM, als auch durch die nach den 12 Ecken desselben führenden Radien OA, am Ikosaeder durch die nach den 12 Ecken führenden Radien OA, jedoch nicht durch die nach den 20 Mittelpunkten seiner Seitenflächen führenden Radien. Nur wenn der Mitte einer Seitenfläche eine Ecke des Polyeders gegenüberliegt, wie beim Tetraeder und beim Sterndodekaeder, bedingen die Radien OM dieselbe Raumeintheilung wie die Radien OA.

Anhang.

VII. Zur Theorie der Gleichungen.

§. 22. Das Lösbarkeitsmerkmal und die Herstellung lösbarer Gleichungen.

1) In den kürzlich veröffentlichten „Beiträgen zur Theorie der Gleichungen“ §. 15 S. 61 habe ich ein allgemeines Merkmal für die Lösbarkeit der Gleichungen, welches von dem Grade der Gleichung unabhängig ist (also nicht eine Primzahl als Grad voraussetzt) angegeben und an der Gleichung dritten Grades $x^3 + a_1 x^2 + a_2 x + a_3 = 0$ erläutert. Ausserdem habe ich das Verfahren zur Aufsuchung der besonderen Formen einer in allgemeiner Form unlösbaren Gleichung n-ten Grades, in welchen sie lösbar wird, ebenfalls an der Gleichung dritten Grades (welche allerdings auch in allgemeiner Form lösbar ist) näher erörtert. Der spezielle Fall, welcher hierbei ins Auge gefasst wurde, ist der einfachste von allen, nämlich derjenige, wo $a_3 = 0$ ist, die kubische Gleichung sich also auf $x^3 + a_1 x^2 + a_2 x = 0$ reduzirt. Ich gestatte mir, nachstehend die Untersuchung der kubischen Gleichung zu erweitern, um damit das fragliche Verfahren noch mehr zu verdeutlichen.

Für die Wurzeln x_1, x_2, x_3 der Gleichung $x^3 + a_1 x^2 + a_2 x + a_3 = 0$ hat man

$$x_1 = b_0 + b_1 + b_2 \qquad \text{also} \quad b_0 = \frac{1}{3}(x_1 + x_2 + x_3)$$

$$x_2 = b_0 + \alpha b_1 + \alpha^2 b_2 \qquad b_1 = \frac{1}{3}(x_1 + \alpha^2 x_2 + \alpha x_3)$$

$$x_3 = b_0 + \alpha^2 b_1 + \alpha b_2 \qquad b_2 = \frac{1}{3}(x_1 + \alpha x_2 + \alpha^2 x_3)$$

worin α die komplexe kubische Wurzel der Einheit, also $\alpha = \sqrt[3]{1}$ und daher $1 + \alpha + \alpha^2 = 0$, $\alpha + \alpha^2 = -1$, $(2\alpha + 1)^2 = -3$, $2\alpha + 1 = \sqrt{-3}$ ist.

Da der Koeffizient $a_1 = -(x_1 + x_2 + x_3)$ ist; so hat man immer $b_0 = -\frac{a_1}{3}$. Die symmetrischen Funktionen der ersten Potenzen der beiden Grössen b_1 und b_2 sind

$$b_1 + b_2 = x_1 - \frac{1}{3}(x_1 + x_2 + x_3)$$

$$b_1 b_2 = \frac{1}{9}[(x_1^2 + x_2^2 + x_3^2) - (x_1 x_2 + x_2 x_3 + x_1 x_3)]$$

Der Werth von $b_1 b_2$ ist eine symmetrische Funktion der Wurzeln x_1, x_2, x_3, der Werth von $b_1 + b_2$ aber nicht. Lässt sich letzterer durch irgend eine Substitution ebenfalls zu einer symmetrischen Funktion gestalten; so ist die spezielle Form der gegebenen Gleichung, welche dieser Substitution entspricht, reduzirbar. Der einfachste ist der schon erwähnte Fall, wo $x_1 = 0$, also $a_3 = 0$ ist. Wir setzen jetzt, zu weiterer Illustration des Verfahrens, $x_2 x_3 = c$, indem wir unter c eine willkürliche rationale Zahl verstehen. Alsdann ist $x_1 = \frac{x_1 x_2 x_3}{c}$, folglich

$$b_1 + b_2 = \frac{x_1 x_2 x_3}{c} - \frac{1}{3}(x_1 + x_2 + x_3)$$

eine symmetrische Funktion. Da $x_1 x_2 x_3 = -a_3$, $x_1 + x_2 + x_3 = -a_1$ und $x_1 x_2 + x_1 x_3 + x_2 x_3 = a_2$ ist; so findet sich leicht $x_1 = -\frac{a_3}{c}$, $x_2 + x_3 = -a_1 + \frac{a_3}{c} = -\frac{(a_2 - c)c}{a_3}$, ferner

$$x_1^2 + x_2^2 + x_3^2 = x_1^2 + (x_2 + x_3)^2 - 2x_2 x_3 = \frac{a_3^2}{c^2} + \frac{(a_1 - c)^2 c^2}{a_3^2} - 2c$$

folglich

$$b_1 + b_2 = \frac{1}{3}\left\{-\frac{2a_3}{c} + \frac{(a_2 - c)c}{a_3}\right\}$$

$$b_1 b_2 = \frac{1}{9}\left\{\frac{a_3^2}{c^2} + \frac{(a_2 - c)^2 c^2}{a_3^2} - a_2 - 2c\right\}$$

Die Werthe von b_1 und b_2 finden sich durch die hieraus sich ergebende quadratische Gleichung, und damit würden auch die Werthe der Wurzeln x_1, x_2, x_3 der kubischen Gleichung bekannt werden, welche, wie leicht zu übersehen, nur Quadratwurzeln, keine Kubikwurzeln enthalten werden. Wir lassen jedoch diese Werthe, welche uns im Augenblicke nicht interessiren, auf sich beruhen und schreiben nur den aus b_0 und $b_1 + b_2$ sich ergebenden Werth

$$b_0 + b_1 + b_2 = \frac{1}{3}\left\{-a_1 - \frac{2a_3}{c} + \frac{(a_2 - c)c}{a_3}\right\}$$

nieder. Da derselbe $= x_1 = -\frac{a_3}{c}$ sein muss; so ergiebt sich die Bedingung $a_1 = \frac{a_3}{c} + \frac{(a_2 - c)c}{a_3}$, welcher die Koeffizienten a_1, a_2, a_3 entsprechen müssen. Setzt man zur Vereinfachung der Formeln $\frac{a_3}{c} = e$ und $a_2 - c = ef$; so hat man $a_1 = e + f$, $a_2 = c + ef$, $a_3 = ce$.

Hierin bezeichnet nicht nur c, sondern auch f (wenn a_1 und a_2 als zwei nicht von vorn herein gegebene, sondern als zwei zu bestimmende Grössen angesehen werden) eine vollkommen willkürliche rationale Zahl. Die letzteren Formeln sagen daher, dass, wenn die kubische Gleichung die Form

$$x^3 + (e+f)x^2 + (c+ef)x + ce = 0$$

hat, worin c und f willkürlich sind, dieselbe durch Quadratwurzeln lösbar ist. Soll das letzte Glied als einfache Zahl a_3 erscheinen; so hat diese Gleichung die Form

$$x^3 + \left(\frac{a_3}{c} + f\right)x^2 + \left(c + \frac{a_3 f}{c}\right)x + a_3 = 0$$

Auch hierin sind c und f willkürliche rationale Zahlen: es versteht sich jedoch von selbst, dass, wenn alle Koeffizienten der Gleichung ganze Zahlen sein sollen, die Grössen c und e im Allgemeinen ganze Zahlen sein müssen.

In der That zerfällt diese kubische Gleichung, wie leicht zu erkennen ist, in eine Gleichung zweiten und ersten Grades, sie wird nämlich

$$(x^2 + fx + c)(x + e) = 0$$

Die Bedingung, welche die Koeffizienten a_1, a_2, a_3 erfüllen müssen, ist, wenn man $\frac{a_3}{c} = -e$ schreibt, identisch mit

$$a_3 + a_2 e + a_1 e^2 + e^3 = 0$$

worin man der Grösse e jeden beliebigen positiven oder negativen Werth geben kann.

Die symmetrische Gleichung $x^3 + ax^2 + ax + 1 = 0$ oder $x^3 - ax^2 - ax + 1 = 0$ oder $x^3 - ax^2 + ax - 1 = 0$ oder $x^3 + ax^2 - ax - 1 = 0$ entspricht immer der vorstehendnn Bedingung, welche jetzt eine der vier Formen $(1 \mp ae)(e^2 \mp 1) = 0$ annimmt. Die symmetrische kubische Gleichung ist daher immer durch Quadratwurzeln lösbar.

2) Von den drei Wurzeln der vorstehenden Gleichung ist die eine x_1 rational und die beiden anderen x_2 und x_3 im Allgemeinen irrational. Die letzteren können nur rational sein, wenn die quadratische Gleichung $x^2 + fx + c = 0$ nur rationale Wurzeln hat, was vermöge einer der vorstehenden ähnlichen Untersuchung für diese quadratische Gleichung die Form $x^2 + (g+h)x + gh = 0$, also für die kubische Gleichung die Form $x^3 + (e+g+h)x^2 + (gh + eg + eh)x + egh = 0$ mit lauter rationalen Werthen von e, g, h verlangt, indem sich dann diese Gleichung in die Gleichung $(x+g)(x+h)(x+e) = 0$ zerlegen lässt. Es würde nicht zulässig sein, die Bedingung für die Rationalität aller drei Wurzeln der kubischen Gleichung direkt aus den allgemeinen Werthen der drei Wurzeln x_1, x_2, x_3 abzuleiten, indem man die Forderung stellte, dass in den allgemeinen Ausdrücken $x_2 = b_0 + ab_2 + a^2 b_2 = b_0 - b_2 + a(b_1 - b_2)$ und $x_3 = b_0 + a^2 b_1 + a b_2 = b_0 - b_1 - a(b_1 - b_2)$ das irrationale Glied durch Annullirung derselben verschwände, was $b_1 = b_2$, also $x_2 = x_3$ verlangen und nur einen speziellen Fall von lauter rationalen Wurzeln ergeben würde. Wenn durch das obige Verfahren die kubische Gleichung

auf die quadratische reduzirt ist, handelt es sich bei der weiteren Untersuchung nicht mehr um eine kubische, sondern um eine quadratische Gleichung, für welche die Bedingungen nicht mehr aus den allgemeinen Werthen von x_1, x_2, x_3, sondern aus den allgemeinen Werthen der Wurzeln x_1, x_2 einer quadratischen Gleichung $x^2 + a_1 x + a_2 = 0$, also aus den Formeln von der Form

$$x_1 = b_0 + b_1 \qquad b_0 = \frac{1}{2}(x_1 + x_2)$$

$$x_2 = b_0 + \alpha b_1 \qquad b_1 = \frac{1}{2}(x_1 + \alpha x_2)$$

worin $\alpha = \sqrt{1} = -1$ ist, abzuleiten sind.

3) Ich hebe hervor, dass die Gleichungen, auf welche sich das in Rede stehende Merkmal der Lösbarkeit bezieht, keineswegs die Abelschen Gleichungen, nämlich diejenigen sind, von welchen jede Wurzel durch jede andere in rationeller Form dargestellt werden kann. Das obige Merkmal ist von einem solchen Zusammenhange ganz unabhängig, schliesst also die Abelschen Gleichungen als spezielle Fälle mit ein. Ausserdem beweis't der §. 5 und 6 der Beiträge zur Theorie der Gleichungen, dass das auf dieses Merkmal gegründete Verfahren auch die allgemeinen Gleichungen des 3-ten und 4-ten Grades lös't, deren Wurzeln nach §. 15 S. 59 jener Beiträge nicht in jenem rationellen Zusammenhange stehen, welche also keine Abelschen Gleichungen sind.

4) Der Ausdruck für $b_1 + b_2$ in voriger Nummer wird für jeden Werth von x_1 symmetrisch, welcher eine symmetrische Funktion darstellt. Setzt man einmal $x_1 = c(x_1 + x_2 + x_3) = -a_1 c$, worin c eine willkürliche Zahl ist; so wird

$$b_1 + b_2 = \left(c - \frac{1}{3}\right)(x_1 + x_2 + x_3) = -a_1\left(c - \frac{1}{3}\right)$$

Die weitere Behandlung führt genau zu derselben Bedingung, welche die Koeffizienten a_1, a_2, a_3 erfüllen müssen, damit die kubische Gleichung in Quadratwurzeln lösbar ist.

Letzteres wird überhaupt der Fall sein, wenn sich ein rationaler Faktor $x - e$ absondern lässt, also wenn die kubische Gleichung eine rationale Wurzel $x_1 = e$ hat, weil dann der zweite Faktor, welcher sich durch Division von $x - e$ in $x^3 + a_1 x + a_2 x + a_3$ ergiebt, eine quadratische Gleichung mit rationalen Koeffizienten liefert. Der gleich null gesetzte Rest dieser Division stellt die allgemeine Bedingung hierfür dar, diese Bedingung ist mithin

$$a_3 + a_2 e + a_3 e^2 + e^3 = 0$$

also der in Nr. 1 gefundenen ganz gleich.

Wir machen bei dieser Gelegenheit die Bemerkung, dass die Fälle, wo sich von einer Gleichung n-ten Grades gleiche oder ungleiche Faktoren niedrigeren Grades (auch für $e = 0$ der Faktor x ein- oder mehreremal) absondern lassen, von der allgemeinen Behandlung dieser Gleichung nicht ausgeschlossen sind, dass also jede Wurzel einer solchen Gleichung einmal in der Form der Wurzeln der Gleichung n-ten Grades, nämlich in der

Form $x = b_0 + \alpha^r b_1 + \alpha^{2r} b_2 + \ldots + \alpha^{(n-1)r} b_{n-1}$ erscheinen kann, dass aber einige dieser Wurzeln zugleich die Form der Wurzel einer Gleichung niedrigeren Grades, nämlich die Form $x = c_0 + \beta^s c_1 + \beta^{2s} c_2 + \ldots + \beta^{(m-1)s} b_{m-1}$ annehmen werden, dass es mithin für jeden Werth von n und m oder für die n-te und m-te Einheitswurzel α und β Funktionen der vorstehenden Form giebt, welche einander gleich sind. In der That, kann jede Grösse e wegen der Beziehung $1 + \alpha + \alpha^2 + \ldots + \alpha^{n-1} = 0$ in die Form $-\alpha e - \alpha^2 e - \alpha^3 e - \ldots - \alpha^{n-1} e$, also in die Form der Wurzel einer Gleichung n-ten Grades gestellt werden, die Wurzel e der Gleichung ersten Grades $x - e = 0$ und überhaupt die Wurzel der Gleichung m-ten Grades kann daher die Form der Wurzel jedes beliebigen Grades n annehmen. Solche Übereinstimmungen setzen jedoch gewisse Beziehungen zwischen den Elementen der übereinstimmenden Wurzelfunktionen, also gewisse Beziehungen zwischen den Koeffizienten der Gleichung, welcher solche Wurzeln angehören, voraus. Die letzteren Beziehungen, welche der gegebenen Gleichung eine spezielle Form verleihen, bilden zugleich die Merkmale für die Zerlegbarkeit jener Gleichung.

Beispielsweise hat die kubische Gleichung $x^3 + a_2 x = 0$ die drei Wurzeln $x_1 = 0$, $x_2 = \alpha \sqrt{\frac{a_2}{3}} - \alpha^2 \sqrt{\frac{2}{3}}$, $x^3 = \alpha^2 \sqrt{\frac{a_2}{3}} - \alpha^2 \sqrt{\frac{a_2}{3}}$, worin α die dritte Einheitswurzel bezeichnet. Die letzten beiden Wurzeln sind aber, wenn β die zweite Einheitswurzel, welche $= -1$ ist, bezeichnet, $x_2 = \sqrt{-a_2}$, $x_3 = \beta \sqrt{-a_2}$ (da $\alpha - \alpha^2 = \sqrt{-3}$ ist), und in der That ist die gegebene Gleichung in der Form $x(x^2 + a_2)$ in eine Gleichung ersten und zweiten Grades zerlegbar.

5) Die Kenntniss eines linearen Faktors $x - x_1$ einer Gleichung n-ten Grades ermöglicht die Reduktion derselben auf den $(n-1)$-ten Grad, und umgekehrt. Da die Gleichung n-ten Grades thatsächlich n Wurzeln hat; so besteht sie auch aus n linearen Faktoren, und es existiren alle Reduktionen auf die Grade $n-1$, $n-2$ u. s. w. Allein, diese n linearen Faktoren und reduzirten Gleichungen, obgleich sie existiren müssen, sind darum doch nicht unbedingt durch endliche algebraische Operationen darstellbar, und demgemäss ist die Gleichung n-ten Grades nicht unbedingt algebraisch lösbar und reduzirbar, und sie heisst nur dann lösbar und reduktibel, wenn sie algebraisch zu lösen oder zu reduziren ist. Es liegt auf der Hand, dass Reduzirbarkeit der gegebenen und jeder reduzirten Gleichung eine unumstössliche Bedingung der Lösbarkeit ist. Möglicherweise kann eine irreduktibele Gleichung, also eine Gleichung, welche nicht die Absonderung eines Faktors ersten Grades (durch algebraische Mittel) gestattet, doch die Absonderung eines Faktors von höherem Grade gestatten. Allerdings würde die Absonderung eines Faktors 2-ten, 3-ten oder 4-ten Grades immer die Absonderung eines Faktors ersten Grades nach sich ziehen, weil die Gleichungen des 2-ten, 3-ten und 4-ten Grades lösbar sind, und demzufolge würde eine Gleichung 5-ten, 6-ten, 7-ten, 8-ten und 9-ten Grades, wenn sie die Absonderung eines Faktors irgend eines Grades gestattete, immer reduzirbar, wenn auch nicht lösbar sein.

Die Zerlegung der Gleichung $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n = 0$ in Faktoren niedrigeren Grades kann auch in Fällen der Unlösbarkeit ein Interesse haben. Setzt man die beiden Faktoren gleich $x^m + c_1 x^{m-1} + c_2 x^{m-2} + \ldots + c_{m-1} x + c_m = 0$ und $x^{n-m} + d_1 x^{n-m-1} + d_2 x^{n-m-2} + \ldots + d_{n-m-1} x + d_{n-m} = 0$ worin $m < n - m$ oder $m < \frac{1}{2} n$ sei; so ergiebt die Ausführung der Multiplikation die n Gleichungen (welche den schon in §. 13 gebrauchten genau entsprechen, wenn man dort die mit dem Zeiger 0 versehenen Koeffizienten $= 1$ setzt)

$$
\begin{aligned}
a_1 &= c_1 + d_1 \\
a_2 &= c_2 + c_1 d_1 + d_2 \\
a_3 &= c_3 + c_2 d_1 + c_1 d_2 + d_3 \\
&\vdots \\
a_m &= c_m + c_{m-1} d_1 + \ldots + c_1 d_{m-1} + d_m \\
a_{m+1} &= c_m d_1 + c_{m-1} d_2 + \ldots + c_1 d_m + d_{m+1} \\
&\vdots \\
a_{n-m} &= c_m d_{n-2m} + c_{m-1} d_{n-2m+1} + \ldots + c_1 d_{n-m-1} + d_{n-m} \\
a_{n-m+1} &= c_m d_{n-2m+1} + c_{m-1} d_{n-2m+2} + \ldots + c_2 d_{n-m-1} + c_1 d_{n-m} \\
&\vdots \\
a_{n-2} &= c_m d_{n-m-2} + c_{m-1} d_{n-m-1} + c_{m-2} d_{n-m} \\
a_{n-1} &= c_m d_{n-m-1} + c_{m-1} d_{n-m} \\
a_n &= c_m d_{n-m}
\end{aligned}
$$

Wenn $m > n - m$ oder $> \frac{1}{2} n$ ist, hat man in diesen Formeln die Buchstaben c und d miteinander zu vertauschen. Wenn für ein paares n die Grösse $m = n - m = \frac{1}{2} n$ ist, nehmen die vorstehenden Formeln dieselbe Gestalt an, wie die durch Vertauschung entstehenden. Übrigens sind alle diese Formeln, mag nun $m >$ oder $<$ oder $= n - m$ sein, in der einzigen Formel

$$a_v = c_v d_0 + c_{v-1} d_1 + c_{v-2} d_2 + \ldots + c_2 d_{v-2} + c_1 d_{v-1} + c_0 d_v$$

enthalten, worin v jeden beliebigen Werth annehmen kann, wenn man beachtet, dass $c_0 = d_0 = 1$, und dass jedes c mit einem höheren Zeiger als m, sowie jedes d mit einem höheren Zeiger als $n - m$ gleich null, dass also c_{m+1}, c_{m+2} u. s. w. $= 0$, d_{n-m+1}, d_{n-m+2} u. s. w. $= 0$ ist.

Die vorstehenden n Gleichungen würden zur Bestimmung der darin enthaltenen n unbekannten Grössen $c_1, c_2, \ldots c_m$ und $d_1, d_2, \ldots d_{n-m}$ ausreichen: die Elimination von $n - 1$ Unbekannten führt jedoch zu einer

Gleichung, welche für die darin verbliebenen Unbekannten mindestens vom n-ten Grade ist, welche also unlösbar ist, wenn $n \geq 5$ ist. Nur für spezielle Fälle ist die gegebene Gleichung zerlegbar. Für diese Zerlegbarkeit lässt sich ein allgemeines Merkmal angeben, welches dem für die Reduzirbarkeit gültigen ähnlich ist: spezielle Fälle, welche die Zerlegung gestatten, ergeben sich übrigens aus der Ermittlung der Bedingungen, unter welchen sich die letzteren n Gleichungen für die darin enthaltenen Unbekannten auflösen lassen.

Die erste der vorstehenden Gleichungen enthält die beiden Unbekannten c_1, d_1, die zweite Gleichung enthält die beiden anderen Unbekannten c_2, d_2, überhaupt jede folgende der erstem m Gleichung zwei neue Unbekannte bis zu dem Paare c_m, d_m. Die dann folgenden $n - 2m$ Gleichungen enthalten immer nur eine neue Unbekannte, nämlich die Grössen d_{m+1}, d_{m+2}, ... d_{n-m}. Die alsdann noch vorhandenen m Gleichungen enthalten keine neuen Unbekannten. Hieraus geht hervor, dass die ersten m Paare von Unbekannten gewisse, durch die beliebig gegebenen Koeffizienten a_1, a_2, ... a_m bestimmten Summen bilden müssen, dass also $c_1 + d_1$, $c_2 + d_2$, ... $c_m + d_m$ die durch die ersten m Koeffizienten a_1, a_2, ... a_m bestimmten Werthe

$$c_1 + d_1 = a_1 \qquad c_2 + d_2 = a_2 - c_1 d_1 \qquad c_3 + d_3 = a_3 - c_2 d_1 - c_1 d_2$$

u. s. w. haben müssen und, dass demzufolge irgend eine der beiden Grössen eines solchen Paares willkürlich angenommen werden kann, dass ferner die $n - 2m$ Unbekannten d_{m+1}, d_{m+2}, ... d_{n-m} gewisse, durch die beliebig gegebenen Koeffizienten a_{m+1}, a_{m+2}, ... a_{n-m} bestimmten Werthe erhalten, dass aber endlich die m Koeffizienten a_{n-m+1}, a_{n-m+2} ... a_n keine beliebigen Werthe haben dürfen, sondern diejenigen Werthe haben müssen, welche den letzten m Gleichungen entsprechen.

Dieses Resultat enthält den Satz: Wenn die ersten $n - m$ Koeffizienten a_1, a_2, ... a_{n-m} einer Gleichung n-ten Grades beliebige gegebene Werthe haben; so lässt sich die Gleichung in einen rationalen Faktor vom Grade m und in einen solchen Faktor vom Grade $n - m$ zerlegen, falls die übrigen m Koeffizienten a_{n-m+1}, a_{n-m+2}, ... a_n die vorstehend bezeichneten Werthe haben. Für $m = 1$ ergiebt sich, dass sich von einer Gleichung n-ten Grades mit $n - 1$ beliebigen Koeffizienten a_1, a_2, ... a_{n-1} ein rationaler linearer Faktor $x + b_1$ absondern lässt, wenn ihr letzter Koeffizient a_n den Werth $c_1 d_{n-1}$ hat. Hierin ist d_{n-1} der letzte Koeffizient des Faktors $(n-1)$-ten Grades, welcher sich durch die Division mit $x + c_1$ in die Funktion $x^n + a_1 x^{n-1} + \ldots + a_n$ ergiebt, also $d_{n-1} = a_{n-1} - a_{n-2} c_1 + a_{n-3} c_1^2 - \ldots \mp c_1^{n-1}$, die Bedingung $a_n = c_1 d_{n-1}$ ist daher gleichbedeutend mit der Bedingung

$$a_n - a_{n-1} c_1 + a_{n-2} c_1^2 - a_{n-3} c_1^3 + \ldots \mp c_1^n = 0$$

oder wenn man den linearen Faktor $x - c$ nimmt, welcher die Wurzel $x = b$ voraussetzt, mit der Bedingung

$$a_n + a_{n-1} c + a_{n-2} c^2 + a_{n-3} c^3 + \ldots + c^n = 0$$

Hieraus, sowie aus dem Vorstehenden geht übrigens hervor, dass in der gegebenen Gleichung $n - 1$ beliebige Koeffizienten willkürlich ange-

nommen werden können und der eine übrig bleibende durch die letzte Gleichung, welche für alle Koeffizienten eine lineare ist, leicht bestimmt werden kann. Die Wurzel c der gegebenen Gleichung hat hierbei die Bedeutung einer willkürlichen Grösse, welcher man jeden beliebigen, auch einen von den Koeffizienten $a_1, a_2, \ldots a_n$ abhängigen rationalen oder irrationalen Werth beilegen kann. Ein irrationaler Werth von b bewirkt im Allgemeinen, dass die Bedingungsgleichung, worin $a_1, a_2, \ldots a_n$ rationale Zahlen sind, in mehrere Bedingungen zerfällt: denn die Rationalität dieser Koeffizienten verlangt mit Nothwendigkeit, dass die Summe aller irrationalen Glieder der letzten Gleichung einen rationalen Werth annimmt, was im Allgemeinen die Annullirung gewisser Theile derselben erfordert.

Betrachten wir beispielsweise die Gleichung 5-ten Grades $x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5 = 0$; so ist dieselbe reduktibel mit der Wurzel

$$
\begin{aligned}
c &= 0 \quad \text{wenn } a_5 = 0\\
c &= 1 \quad \text{„ } a_5 + a_4 + a_3 + a_2 + a_1 + 1 = 0\\
c &= -1 \quad \text{„ } a_5 - a_4 + a_3 - a_2 + a_1 - 1 = 0\\
c &= \sqrt{e} \quad \text{„ } a_5 + a_4\sqrt{e} + a_3 e + a_2 e\sqrt{e} + a_1 e^2 + e^2\sqrt{e} = 0\\
c &= \sqrt[3]{e} \quad \text{„ } a_5 + a_4 e^{\frac{1}{3}} + a_3 e^{\frac{2}{3}} + a_2 e + a_1 e e^{\frac{1}{3}} + e e^{\frac{2}{3}} = 0\\
c &= \sqrt[4]{e} \quad \text{„ } a_5 + a_4 e^{\frac{1}{4}} + a_3 e^{\frac{2}{4}} + a_2 e^{\frac{3}{4}} + a_1 e + e e^{\frac{1}{4}} = 0\\
c &= \sqrt[5]{e} \quad \text{„ } a_5 + a_4 e^{\frac{1}{5}} + a_3 e^{\frac{2}{5}} + a_2 e^{\frac{3}{5}} + a_1 e^{\frac{4}{5}} + e = 0\\
c &= \sqrt[6]{e} \quad \text{„ } a_5 + a_4 e^{\frac{1}{6}} + a_3 e^{\frac{2}{6}} + a_2 e^{\frac{3}{6}} + a_1 e^{\frac{4}{6}} + e^{\frac{5}{6}} = 0
\end{aligned}
$$

Damit die Gleichung 5-ten Grades eine irrationale Quadratwurzel $\sqrt{e}$ aus einer rationalen Zahl e zur Wurzel haben könne, muss also $a_4\sqrt{e} + a_2 e\sqrt{e} + e^2\sqrt{e} = (a_4 + a_2 e + e^2)\sqrt{e}$ einen rationalen Werth haben, was nur möglich ist, wenn $a_4 + a_2 e + e^2 = 0$ ist. Die Bedingung zerfällt daher in die beiden Bedingungsgleichungen

$$a_4 + a_2 e + e^2 = 0 \qquad a_5 + a_3 e + a_1 e^2 = 0$$

wodurch zwei Koeffizienten durch die übrigen drei bestimmt werden, indem man z. B. für a_4 und a_5 die Ausdrücke $a_4 = -a_2 e - e^2$ und $a_5 = -a_3 e - a_1 e^2$ setzen kann. Im Übrigen kann man durch Elimination von e auch eine Beziehung zwischen den fünf Koeffizienten herstellen, muss dann aber für e den durch Auflösung der einen oder anderen Bedingungsgleichung sich ergebenden Werth annehmen.

Eine irrationale Kubikwurzel $\sqrt[3]{e}$ als Wurzel der Gleichung 5-ten Grades verlangt, dass

$$a_4 e^{\frac{1}{3}} + a_3 e^{\frac{2}{3}} + a_1 e e^{\frac{1}{3}} + e e^{\frac{2}{3}} = \left[a_4 + a_1 e + (a_3 + e) e^{\frac{1}{3}}\right] e^{\frac{1}{3}}$$

einen rationalen Werth habe, also $a_4 + a_1 e + (a_3 + e) e^{\frac{1}{3}} = 0$, mithin

$(a_1 + e)\,e^{\frac{1}{3}}$ rational, folglich $a_3 + e = 0$ sei. Hierdurch ergeben sich die drei Bedingungsgleichungen

$$a_3 + e = 0 \qquad a_4 + a_1 e = 0 \qquad a_5 + a_2 e = 0$$

welche auch

$$a_3 = -e \qquad a_4 = a_1 a_3 \qquad a_5 = a_2 a_3$$

geschrieben werden können.

Eine irrationale Wurzel vierten Grades als Wurzel der Gleichung fünften Grades führt zu den vier Bedingungsgleichungen

$$a_2 = 0 \qquad a_3 = 0 \qquad a_4 + e = 0 \qquad a_5 + a_1 e = 0$$

wofür man auch

$$a_2 = 0 \qquad a_3 = 0 \qquad a_4 = -e \qquad a_5 = a_1 a_4$$

setzen kann. Die gegebene Gleichung muss hiernach die Form $x_5 + a_1 x^4 + a_4 x + a_1 a_4 = 0$ haben und ihre Wurzel wird $= \sqrt[4]{-a_4}$ sein.

Eine irrationale Wurzel fünften Grades als Wurzel der Gleichung fünften Grades ergiebt die fünf Bedingungsgleichungen

$$a_1 = 0 \qquad a_2 = 0 \qquad a_3 = 0 \qquad a_4 = 0 \qquad a_5 = -e$$

wodurch sich die gegebene Gleichung auf die binomische Gleichung $x^5 + a_5 = 0$ reduzirt, welche in der That die Wurzel $\sqrt[5]{-a_5}$ hat.

Eine irrationale Wurzel sechsten Grades als Wurzel der Gleichung fünften Grades nöthigt zu den sechs Beziehungen

$$a_1 = 0 \qquad a_2 = 0 \qquad a_3 = 0 \qquad a_4 = 0 \qquad a_5 = 0 \qquad e = 0$$

wodurch die gegebene Gleichung die Form $x^5 = 0$ annimmt, welche zwar die Wurzel $x = \sqrt[6]{e} = \sqrt[6]{0} = 0$ hat, aber doch die Forderung, dass diese Wurzel eine irrationale Wurzel sechsten Grades sei, nicht erfüllt. In der That, ist es unmöglich, dass eine Gleichung n-ten Grades mit lauter rationalen Koeffizienten $a_1, a_2, \ldots a_n$ eine Wurzel habe, welche eine irrationale Wurzel von höherem als dem n-ten Grade darstelle. Auch die binomische Gleichung $x^n + a_n = 0$, deren Wurzeln sämmtlich durch $x = (-a_n)^{\frac{1}{n}}$ dargestellt sind, kann, wenn a_n und e rational sind, keine irrationale Wurzel von der Form $e^{\frac{1}{n+m}}$ haben, da $-a_n$ nicht $= e^{n+m}$ sein kann.

Nach den im Eingange dieser Nummer aufgestellten Formeln können die Werthe aller Koeffizienten d von d_1 bis d_{n-m} als Funktionen der Koeffizienten $a_1, a_2, \ldots a_{n-m}$ und der Koeffizienten $c_1, c_2, \ldots c_m$ dargestellt werden: man hat

$$\begin{aligned} d_1 &= a_1 - c_1 \\ d_2 &= a_2 - a_1 c + (c_1^2 - c_2) \\ d_3 &= a_3 - a_2 c_1 + a_1 (c_1^2 - c_2) - (c_1^3 - 2 c_1 c_2) \end{aligned}$$

u. s. w. Substituirt man diese Werthe der d, welche ausser den Koeffizienten a nur die Koeffizienten c enthalten, in die Ausdrücke für die m Koeffizienten a_{n-m+1}, a_{n-m+2}, . . . a_n; so stellen sich in dieser Form die m Bedingungsgleichungen dar, welche erfüllt werden müssen, damit die Gleichung vom n-ten Grade in zwei Gleichungen vom Grade m und $n - m$ und zwar in die beiden Gleichungen mit den Koeffizienten c_1, c_2, . . . c_m bezw. d_1, d_2, . . . d_{n-m} zerlegt werden kann. So beantwortet sich z. B. die Frage der Zerlegung der Gleichung 5-ten Grades in eine Gleichung vom Grade $m = 2$ und $n - m = 3$ vermittelst der Formeln

$$\begin{aligned} a_1 &= c_1 + d_1 && \text{also } d_1 = a_1 - c_1 \\ a_2 &= c_2 + c_1 d_1 + d_2 && d_2 = a_2 - a_1 c_1 + c_1^2 - c_2 \\ a_3 &= c_2 d_1 + c_1 d_2 + d_3 && d_3 = a_3 - a_2 c_1 + a_1 (c_1^2 - c_2) - (c_1^3 - 2 c_1 c_2) \\ a_4 &= c_2 d_2 + c_1 d_3 \\ a_5 &= c_2 d_3 \end{aligned}$$

indem man die aus den ersten drei Gleichungen sich ergebenden Werthe von d_2 und d_3 in die Ausdrücke für a_4 und a_5 einsetzt, wobei c_1 und c_2 willkürlich bleiben. Ist die gegebene Gleichung eine abgekürzte, also $a_1 = 0$; so vereinfachen sich die Formeln dementsprechend. Setzt man einmal für die verkürzte Gleichung fünften Grades $c_1 = c_2 = 1$; so wird $d_1 = -1$, $d_2 = a_2$, $d_3 = a_3 - a_2 + 1$ und die beiden Bedingungsgleichungen $a_4 = a_3 + 1$, $a_5 = a_3 - a_2 + 1$, d. h. man hat

$$\begin{aligned} &x^5 + a_2 x^3 + a_3 x^2 + (a_3 + 1) x + (a_3 - a_2 + 1) \\ &= (x^2 + x + 1)(x^3 - x^2 + a_2 x + a_3 - a_2 + 1) \end{aligned}$$

Wenn behuf Herstellung der Werthe der Koeffizienten c und d die Auflösung der im Anfange dieser Nummer aufgestellten Gleichungen von unten nach oben bewirkt wird; so ergiebt die unterste oder n-te Gleichung für das Produkt der beiden Koeffizienten c_m und d_{n-m} den Werth $c_m d_{n-m} = a_n$, darauf lieferte die $(n - 1)$-te Gleichung die Beziehung zwischen c_{m-1} und d_{n-m-1} u. s. f.

Hat man kein Interesse an der Kenntniss der Beziehungen zwischen den Grössen c und d; so ergeben sich die Bedingungsgleichungen für die Koeffizienten des einen Faktors, z. B. für c_1, c_2, . . . c_m durch Division mit $x^m + c_1 x^{m-1} + \ldots + c_m$ in die Funktion $x^n + a_1 x^{n-1} + \ldots + a_n$, bis sich der Rest vom Grade $m - 1$ in der Form der Funktion $A_1 x^{m-1} + A_2 x^{m-2} + \ldots + A_{m-1} x + A_m$ einstellt. Dieser Rest muss $= 0$ sein. Da aber x, als Wurzel einer Gleichung n-ten Grades, n verschiedene Werthe hat, die durch Annullirung des Restes sich ergebende Gleichung $(m - 1)$-ten Grades aber nur $m - 1$ Werthe für x ergeben könnte; so zieht die letztere Forderung die m Bedingungsgleichungen

$$A_1 = 0, \quad A_2 = 0, \quad \ldots \quad A_{m-1} = 0, \quad A_m = 0$$

nach sich, welche sofort das Resultat der Elimination der Grössen d aus den vorstehend durch die c und d ausgedrückten Beziehungen darstellt.

6) Was die Zerlegbarkeit der allgemeinen Gleichung n-ten Grades betrifft; so ist dieselbe, da sie die Auflösung einer allgemeinen Gleichung des n-ten oder eines höheren Grades erfordert, für jede Gleichung, deren Grad höher ist, als der vierte, unmöglich. Von der allgemeinen Gleichung 5-ten, 6-ten, 7-ten ... Grades kann weder ein Faktor 1-sten, noch 2-ten, noch 3-ten, noch irgend eines anderen Grades abgesondert werden. Die den 4-ten Grad übersteigenden Gleichungen sind nur dann spaltbar, wenn ihre Koeffizienten gewisse speziellen und zwar solche Werthe haben, welche den vorstehenden Bedingungen entsprechen, insofern diese Bedingungen algebraisch realisirbar sind, d. h. insofern die gegebenen Daten derartig beschaffen sind, dass sie nicht die Auflösung einer allgemeinen Gleichung vom 5-ten oder höherem Grade erfordern. Unter diesem Gesichtspunkte, nämlich unter Vermeidung allgemeiner Gleichungen 5-ten oder höheren Grades, regelt sich die Behandlung der obigen Bedingungsgleichungen durch ein Verfahren, welches wir zunächt an der Absonderung eines Faktors ersten Grades $x + c$ von der Gleichung 5-ten Grades $x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5 = 0$ erläutern wollen. Die Bedingungsgleichung, welche die Koeffizienten a_1, a_2, a_3, a_4, a_5 erfüllen müssen, ist

$$c^5 - a_1 c^4 + a_2 c^3 - a_3 c^2 + a_4 c - a_5 = 0$$

Sieht man c als Willkürliche an; so liefert diese für a_1, a_2, a_3, a_4, a_5 lineare Gleichung den Werth für irgend einen dieser Koeffizienten, während alle übrigen, sowie die Grösse c beliebig gegebene Werthe haben können.

Fasst man, um zu einer anderen Auflösung zu gelangen, irgend zwei, etwa die beiden höchsten Glieder $c^5 - a_1 c^4$ in ein einziges Glied $(c - a_1) c^4$ zusammen und setzt den Faktor $c - a_1 = f_1$, indem man nunmehr nicht c, sondern f_1 als die Willkürliche betrachtet, von welcher c durch die Beziehung $c = f_1 + a_1$ abhängt; so hat man statt der einen Bedingungsgleichung, welche für c vom 5-ten Grade ist, zwei Bedingungsgleichungen, welche für c vom 1-sten und 4-ten Grade sind, nämlich die beiden Gleichungen

$$f_1 = c - a_1 \quad \text{und} \quad f_1 c^4 + a_2 c^3 - a_3 c^2 + a_4 c - a_5 = 0$$

Setzt man den Werth $c = f_1 + a_1$ aus der ersten in die zweite Bedingungsgleichung; so ergiebt sich

$$f_1 (f_1 + a_1)^4 + a_2 (f_1 + a_1)^3 - a_3 (f_1 + a_1)^2 + a_4 (f_1 + a_1) - a_5 = 0$$

als die Beziehung, welche durch die Koeffizienten a_1, a_2, a_3, a_4, a_5 erfüllt werden muss. Der sich absondernde Faktor ersten Grades ist dann $x + c = x + f_1 + a_1$. In diesen Formeln ist f_1 vollkommen willkürlich. Nähme man beispielsweise $f_1 = 0$; so würde $a_2 a_1^3 - a_3 a_1^2 + a_4 a_1 - a_5 = 0$, also $a_5 = a_1 (a_1^2 a_2 - a_1 a_3 + a_4)$ sein müssen. Von der Gleichung 5-ten Grades

$$x^5 + a_2 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_1 (a_1^2 a_2 - a_1 a_3 + a_4) = 0$$

lässt sich dann der Faktor $x + a_1$ absondern.

Wäre die gegebene Gleichung 5-ten Grades eine verkürzte, also $a_1 = 0$; so würde die letztere Substitution sagen, dass x ein Faktor von $x^5 + a_2 x^3 + a_3 x^2 + a_4 x = 0$ sei, was selbstverständlich ist

Nähme man für die verkürzte Gleichung 5-ten Grades $c_5 + a_2 c^3 = (c^2 + a_2) c^3 = f_1 c^3$; so fände man $a_2 = f_1 - c^2$ und $a_5 = a_4 c - a_3 c^2 = a_4 \sqrt{f_1 - a_2} - a_3 (f - a_2)$. Für $f_1 = 0$ wird $a_2 = -c^2$ und $a_5 = a_4 c - a_3 c^2$, die Gleichung $x^5 - c^2 x^3 + a_3 x^2 + a_4 x + a_4 c - a_3 c^2 = 0$ hat also den Faktor $x + c$.

Eine andere Auflösung ergiebt sich durch Zusammenfassung von drei Gliedern der ursprünglichen Bedingungsgleichung, etwa der ersten drei in der Form

$$c^5 - a_1 c^4 + a_2 c^3 = (c^2 - a_1 c + a_2) c^3 = f_2 c^3$$

Indem man als erste Bedingungsgleichung $c^2 - a_1 c + a_2 = f_2$ setzt; so hat man als zweite Bedingungsgleichung

$$f_2 c^3 - a_3 c^2 + a_4 c - a_5 = 0$$

Die erste Bedingungsgleichung ist jetzt eine quadratische; ihre Auflösung für c ergiebt

$$c = \frac{a_1}{2} \mp \sqrt{f_2 - a_2 + \frac{a_1^2}{4}}$$

Wird dieser Werth in die zweite Bedingungsgleichung gesetzt; so erhält man eine Beziehung zwischen den Koeffizienten a_1, a_2, a_3, a_4, a_5 und der Willkürlichen f_2. Wählt man diese Willkürliche so, dass $f_2 - a_2 + \frac{a_1^2}{4}$ das Quadrat einer rationalen Zahl p wird, d. h. setzt man $f_2 = p^2 + a_2 - \frac{a_1^2}{4}$; so wird sowohl c, als auch die zweite Bedingungsgleichung rational, und wegen der Zweiwerthigkeit der Wurzelgrösse ergeben sich die Bedingungsgleichungen für zwei verschiedene Auflösungen. Im Allgemeinen, d. h. für einen beliebigen Werth von f_2 scheidet sich der Ausdruck auf der linken Seite der zweiten Bedingungsgleichung in einen rationalen und in einen irrationalen Theil, welcher letztere das Produkt eines rationalen Faktors und der Grösse $\sqrt{f_2 - a_2 + \frac{a_1^2}{4}}$ ist. Demgemäss zerfällt die zweite Bedingungsgleichung durch Annullirung dieser beiden Theile in zwei Beziehungen, welche die Koeffizienten a erfüllen müssen: die eine ergiebt unmittelbar den Werth von a_5, die andere den von a_4 und der abzusondernde lineare Faktor $x + c$ wird irrational und zweiwerthig, während die Koeffizienten a sämmtlich rational bleiben.

In ähnlicher Weise gelangt man durch Zusammenfassung von vier Gliedern zu der Auflösung, nach welcher c die Wurzel einer kubischen Gleichung ist, und durch Zusammenfassung von fünf Gliedern zu der Auflösung, nach welcher c die Wurzel einer biquadratischen Gleichung ist.

Das vorstehende Verfahren zur Aufstellung der Beziehungen, welche die Koeffizienten a der gegebenen Gleichung erfüllen müssen, damit sich ein Faktor ersten Grades absondern, also die Gleichung reduziren lässt, kann offenbar auf die Gleichung jeden Grades n angewandt werden: es können jedoch im Allgemeinen nicht mehr als die fünf ersten Glieder zusammengefasst, also keine allgemeinen Werthe von c erwartet

werden, welche Wurzeln von Gleichungen 5-ten oder höheren Grades darstellen. Um solche Werthe von c zu erhalten, muss die Zusammenfassung von mehr als fünf Gliedern eine auflösbare, also reduzibele Gleichung 5-ten oder höheren Grades ergeben. Demzufolge ist an die sich ergebende Bedingungsgleichung, wenn sie den gedachten Zweck erfüllen soll, zunächst die Forderung der Zerlegbarkeit zu stellen. Diese Forderung wird, wenn die Bedingungsgleichung vom 5-ten Grade ist, durch das vorstehende Verfahren, wenn sie vom 6-ten Grade ist, durch das zur Abtrennung eines Faktors 2-ten Grades dienende Verfahren, wenn sie vom 7-ten Grade ist, durch das zur Abtrennung eines Faktors 3-ten Grades dienende Verfahren, und sie wird generell erfüllt werden können, wenn das Verfahren für die Absonderung eines Faktors 2-ten, 3-ten und 4-ten Grades erläutert sein wird, d. h. man kann alsdann die Bedingungen formuliren, welche die rationalen Koeffizienten einer Gleichung n-ten Grades zu erfüllen haben, damit sich von dieser Gleichung ein linearer Faktor $x + c$ absondern lässt, worin c rational oder irrational, nämlich die Wurzel einer Gleichung 1-sten, 2-ten, ... n-ten Grades ist. Diese Erläuterung enthält aber zugleich die Entwicklung des Verfahrens, welches zur Absonderung eines Faktors von beliebigem Grade m mit rationalen und irrationalen Koeffizienten $c_1, c_2, \ldots c_m$ dient.

Was nun die Absonderung eines Faktors m-ten Grades $x^m + c_1 x^{m-1} + c_2 x^{m-2} + \ldots + c_m$ betrifft; so ergeben sich nach Nr. 5 m Bedingungsgleichungen, in welchen die Produkte der Grössen $c_1, c_2, \ldots$ und ihre Potenzen (jedoch keine der Grössen $d_1, d_2, \ldots$) erscheinen. Sieht man alle diese Grössen c als Willkürliche an; so lassen sich aus jenen Bedingungsgleichungen, welche für die Koeffizienten $a_1, a_2, \ldots$ linear sind, m der Letzteren bestimmen, wenn $n - m$ derselben willkürlich angenommen werden.

Nimmt man nun nicht alle c oder keins derselben, sondern gewisse Funktionen derselben, welche Faktoren irgend einer Anzahl von Gliedern der Bedingungsgleichungen bilden, als die Willkürlichen $f_1, f_2, \ldots$ an; so kann man diese Funktionen, welche durch $k_1 F_1, k_2 F_2, \ldots$ bezeichnet sein mögen, immer so wählen, dass sich das System der Gleichungen $F_1 = f_1, F_2 = f_2$ u. s. w. für diejenigen darin enthaltenen Grössen c, welche den Charakter der Willkürlichkeit verlieren sollen, auflösen lässt. Die sich durch diese Auflösungen ergebenden Werthe der betreffenden c werden dann nur die Willkürlichen $f_1, f_2, \ldots$ und diejenigen Koeffizienten c, welche den Charakter der Willkürlichkeit beibehalten sollen, ausserdem aber nur die Koeffizienten $a_1, a_2, \ldots a_{n-m}$, jedoch keinen der Koeffizienten $a_{n-m+1}, a_{n-m+2}, \ldots a_n$ enthalten. Substituirt man diese Werthe der betreffenden c in die Bedingungsgleichungen; so erhält man m Beziehungen zwischen den Koeffizienten $a_1, a_2, \ldots a_n$, welche ausser diesen Grössen nur Willkürliche enthalten, und welche auch stets realisirt werden können, weil eine jede derselben einen einzigen der Koeffizienten $a_{n-m+1}, a_{n-m+2}, \ldots a_n$ auf erster Potenz als einzelnes Glied enthält.

Will man beispielsweise die Abtrennung eines quadratischen Faktors $x^2 + c_1 x + c_2$ von der Gleichung fünften Grades untersuchen; so kann man einmal in den in Nr. 5 aufgestellten Gleichungen für a_4 und a_5, nachdem darin für d_2 und d_3 ihre Werthe in c_1 und c_2 substituirt sind,

$a_1 c_1^3 - c_1^4 = c_1^3 (a_1 - c_1)$, also $a_1 - c_1 = f_1$ und daher $c_1 = a_1 - f_1$ setzen, indem man f_1 und c_2 als zwei Willkürliche ansieht. Eine Substitution dieses Werthes von c_1 in die beiden Gleichungen für a_4 und a_5 ergeben dann sofort die durch beliebige Werthe von a_1, a_2, a_3, c_2, f_1 dargestellten Werthe der beiden Koeffizienten a_4 und a_5, welche die Gleichung fünften Grades in verlangter Weise spaltbar machen.

Man könnte auch ausser dieser Substitution noch $2 c_1 c_2^2 - a_2 c_1 c_2 = c_1 c_2 (2 c_2 - a_2)$, also $2 c_2 - a_2 = f_2$ und daher $c_2 = \frac{1}{2} (a_2 + f_2)$ setzen, wodurch die Werthe von a_4 und a_5 von den beiden Willkürlichen f_1 und f_2 abhängig werden.

Soll zwischen c_1 und c_2 eine gegebene Beziehung bestehen, soll etwa der quadratische Faktor zwei gleiche Wurzeln, also die Form $x^2 + 2 c x + c^2$ haben, sodass $c_1 = 2 c$ und $c_2 = c^2$ ist; so findet sich

$$a_4 = 2 a_3 c - 3 a_2 c^2 + 4 a_1 c^3 - 5 c^4$$
$$a_5 = a_3 c^2 - 2 a_2 c^3 + 3 a_1 c^4 - 4 c^5$$

worin c willkürlich bleibt.

7) Die möglichen Substitutionen, welche zu machen sind, um von einer Gleichung n-ten Grades einen Faktor m-ten Grades abzusondern, bieten eine grosse Mannichfaltigkeit dar: gleichwohl ist ihre Anzahl eine begrenzte, und daraus folgt, dass es nur eine endliche Menge von Formen der Gleichung n-ten Grades geben kann, welche die Absonderung eines Faktors m-ten Grades gestatten. Im Vorstehenden ist zugleich der Weg gezeigt, welcher einzuschlagen ist, um alle diese Formen herzustellen: es handelt sich dabei um die nach Nr. 5 stets mögliche Aufstellung der m Bedingungsgleichungen, welche nach Ausscheidung aller d nur die m Grössen $c_1, c_2, \ldots c_m$ enthalten. Erweis't sich dieses System von Gleichungen für alle darin enthaltenen Unbekannten c auflösbar, d. h. führt die Elimination von $m - 1$ dieser Unbekannten zu einer Gleichung, welche für irgend eine Potenz der darin enthaltenen einen Unbekannten höchstens vom vierten Grade ist; so können alle Koeffizienten c, also der gesuchte Faktor m-ten Grades hergestellt werden, welche Werthe auch die Koeffizienten a der gegebenen Gleichung n-ten Grades haben mögen. Dieses Ergebniss kann jedoch nur eintreten, wenn der Grad n der gegebenen Gleichung den vierten nicht überschreitet. Ist $n \geqq 5$; so ist das System der m Bedingungsgleichungen nur durch Substitutionen darstellbar, wodurch spezielle Beziehungen zwischen den Koeffizienten $a_1, a_2, \ldots a_n$ der gegebenen Gleichung gestiftet werden. Diese Beziehungen, also die möglichen Formen der Gleichung, welche die Absonderung eines Faktors m-ten Grades gestatten, sind nach Obigem sämmtlich darstellbar, mithin die in der Auffindung der Formen der zerlegbaren Gleichung n-ten Grades bestehende Aufgabe durch Vorstehendes vollständig gelös't.

8) Es ist beachtenswerth, dass in den im Eingange von Nr. 5 aufgestellten Gleichungen die Grössen $a_1, a_2, \ldots a_n$ die Bedeutung der symmetrischen Grundfunktionen der Wurzeln $x_1, x_2, \ldots x_n$ haben. Bezeichnet man also mit ${}^s\Phi_t$ die symmetrische Grundfunktion von der Dimensität s aus t Elementen, sodass ${}^1\Phi_n = x_1 + x_2 + \ldots + x_n$,

$^2\Phi_n = x_1 x_2 + x_1 x_3 + x_2 x_3 + \ldots$ ist (vgl. §. 1 der Beiträge zur Theorie der Gleichungen); so ist $a_1 = -\,{}^1\Phi_n$, $a_2 = +\,{}^2\Phi_n$, $a_3 = -\,{}^3\Phi_n$ u. s. w. Die Grössen $c_1, c_2, \ldots c_m$ haben die Bedeutung von $-\,{}^1\Phi_m$, $+\,{}^2\Phi_m$, $-\,{}^3\Phi_m$ u. s. w. und die Grössen $d_1, d_2, \ldots d_r$, worin $r = n - m$ ist, die Bedeutung von $-\,{}^1\Phi_r$, $+\,{}^2\Phi_r$, $-\,{}^3\Phi_r$ u. s. w. Da die Funktionen von gleicher Dimensität ohne Rücksicht auf die Elementenzahl n, m, r dasselbe Zeichen haben; so kann man in den gedachten Formeln ohne Weiteres ${}^s\Phi_n$ an die Stelle von a_s, ${}^s\Phi_m$ an die Stelle von c_s und ${}^s\Phi_r$ an die Stelle von d_s setzen. Man hat also die Beziehungen

$$a_1 = {}^1\Phi_n = {}^1\Phi_m + {}^1\Phi_r$$
$$a_2 = {}^2\Phi_n = {}^2\Phi_m + {}^1\Phi_r\,{}^1\Phi_m + {}^2\Phi_r$$

u. s. w., allgemein

$$a_v = {}^v\Phi_n = {}^v\Phi_m\,{}^0\Phi_r + {}^{v-1}\Phi_m\,{}^1\Phi_r + {}^{v-2}\Phi_m\,{}^2\Phi_r + \ldots + {}^1\Phi_m\,{}^{v-1}\Phi_r + {}^0\Phi_m\,{}^v\Phi_r$$

wenn man hierin ${}^0\Phi_m = {}^0\Phi_r = 1$ und jedes ${}^s\Phi_m$ von höherer Dimensität s als die m-te, sowie jedes ${}^s\Phi_r$ von höherer Dimensität s als die r-te gleich null setzt.

Die Beziehung zu den symmetrischen Funktionen der Wurzeln gewährt das Mittel, die Bedingungen für die Abtrennung eines Faktors m-ten Grades von einer Gleichung n-ten Grades auf einem anderen Wege abzuleiten. Zu dem Ende bringen wir in Erinnerung, dass, wenn ${}^s_r\Phi_m$ die s-dimensionale symmetrische Grundfunktion der r-ten Potenzen der m Elemente $x_1, x_2, \ldots x_m$, also der Elemente $x_1^r, x_2^r, \ldots x_m^r$ bezeichnet, diese Grösse nach der Theorie der symmetrischen Funktionen eine leicht darstellbare ganze rationale Funktion der Potenzen der einfachen symmetrischen Funktionen $-\,{}^1_1\Phi_m = c_1$, $+\,{}^2_1\Phi_m = c_2$, $\ldots (-1)^n\,{}^m_1\Phi_m = c_m$ ist. Wir drücken Diess kurz durch die Formeln

$${}^1_r\Phi_m = F_1(c),\quad {}^2_r\Phi_m = F_2(c),\quad \ldots\quad {}^m_r\Phi_m = F_m(c)$$

aus.

Sind nun $x_1, x_2, \ldots x_m$ die m Wurzeln der Gleichung n-ten Grades $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, welche dem Faktor $x^m + c_1 x^{m-1} + \ldots + c_m = 0$ angehören; so bestehen die m Gleichungen

$$x_1^n + a_1 x_1^{n-1} + \ldots + a_n = 0$$
$$x_2^n + a_1 x_2^{n-1} + \ldots + a_n = 0$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$x_m^n + a_1 x_m^{n-1} + \ldots + a_n = 0$$

Addirt man erst diese Gleichungen, sodann die Produkte von je zwei, je drei ... derselben und bildet zuletzt das Produkt aller; so erhält man m Gleichungen, welche ganze rationale Funktionen der m Grössen $c_1, c_2, \ldots c_m$ und der n Koeffizienten $a_1, a_2, \ldots a_n$ sind. Diese m Bedingungsgleichungen sind mit den obigen ganz identisch. Wenn sie lösbar sind, können daraus m Grössen bestimmt werden, während n Grössen

willkürlich bleiben. Sieht man die n Koeffizienten $a_1, a_2, \ldots a_n$ der gegebenen Gleichung als die willkürlich gegebenen Grössen an, setzt man also eine allgemeine Gleichung n-ten Grades voraus; so würden die m Bedingungsgleichungen, wenn sie lösbar sind, wenn also die Elimination von $m-1$ der Grössen c auf eine Gleichung 4-ten oder niedrigeren Grades führt, die gesuchten Koeffizienten $c_1, c_2, \ldots c_m$ des Faktors m-ten Grades liefern, wenn sie aber unlösbar sind, wie es für jeden Werth von $n \geq 5$ sicher der Fall ist, machen sie die Absonderung eines Faktors jeden, auch ersten Grades unmöglich. Die Absonderung eines Faktors von einer höheren Gleichung ist also nur möglich, wenn nicht alle Koeffizienten a der gegebenen Gleichung willkürliche Werthe haben, d. h. wenn zwischen diesen Koeffizienten eine Beziehung besteht, welche der gegebenen Gleichung den Charakter einer allgemeinen Gleichung entzieht und ihr den einer speziellen Gleichung verleihet. Wenn von diesen Koeffizienten a eine bestimmte Anzahl r willkürlich gegebene Grössen sind, können die übrigen $n-r$ und daneben $r+m-n$ der Grössen c aus den Bedingungsgleichungen bestimmt werden, während $n-r$ der Grössen c willkürlich bleiben, vorausgesetzt, dass die m Bedingungsgleichungen für die fraglichen Grössen a und c auflösbar sind. Diese Auflösbarkeit kann nach Obigem durch die Einführung neuer Willkürlichen f herbeigeführt werden. Die Gesammtzahl von n Willkürlichen und m zu bestimmenden Grössen ändert sich durch die Einführung dieser neuen Willkürlichen f nicht: die Zerlegung einer Gleichung vom 5-ten oder höheren Grade oder die spezielle Form, welche eine solche Zerlegung möglich macht, ist daher (weil der Fall, dass die n Koeffizienten $a_1, a_2, \ldots a_n$ die Willkürlichen seien, ausgeschlossen ist), von einer oder mehreren Willkürlichen f abhängig, während die übrigen nothwendig erforderlichen Willkürlichen den Grössen c angehören. Es giebt also immer unendlich viel zerlegbare Gleichungen von derselben Form.

Soll eine Gleichung n-ten Grades denselben Faktor m-ten Grades $x^m + c_1 x^{m-1} + c_2 x^{m-2} + \ldots$ haben wie eine Gleichung n'-ten Grades; so müssen die Grössen $c_1, c_2, \ldots$ in den m Bedingungsgleichungen der einen wie in denen der anderen Gleichung dieselben Werthe haben. Diess führt zu den Bedingungen, unter welchen zwei Gleichungen ein gemeinschaftliches Maass haben.

9) Die Bedingungen für die Lösbarkeit einer Gleichung n-ten Grades bilden das System der n Bedingungen, unter welchen sich von der gegebenen Gleichung ein linearer Faktor $x + c_1$, sodann von der nach Absonderung dieses Faktors sich ergebenden Gleichung $(n-1)$-ten Grades $x^{n-1} + d_1 x^{n-2} + d_2 x^{n-3} + \ldots + d_{n-1} = 0$, worin $d_1 = a_1 - c_1$, $d_2 = a_2 - a_1 c_1 + c_1^2$, $d_3 = a_3 - a_2 c_1 + a_1 c_1^2 - a_1 c_1^3$ u. s. w. ist, wiederum ein linearer Faktor $x + c_2$, welcher die Gleichung $x^{n-2} + e_1 x^{n-3} + e_2 x^{n-4} + \ldots + e_{n-2} = 0$ zurücklässt, u. s. w. absondern lässt. Die Koeffizienten d, e, f u. s. w. bestimmen sich durch die Rekursionsformeln

$$d_1 = a_1 - c_1 \quad d_2 = a_2 - a_1 c_1 + c_1^2 \quad d_3 = a_3 - a_2 c_1 + a_1 c_1^2 - c_1^3 \ldots$$
$$e_1 = d_1 - c_2 \quad e_2 = d_2 - d_1 c_2 + c_2^2 \quad e_3 = d_3 - d_2 c_2 + d_1 c_2^2 - c_2^3 \ldots$$
$$f_1 = e_1 - c_3 \quad f_2 = e_2 - e_1 c_3 + c_3^2 \quad f_3 = e_3 - e_2 c_3 + e_1 c_3^2 - c_3^3 \ldots$$

u. s. w., und die n Bedingungsgleichungen sind

$$a_n - a_{n-1} c_1 + a_{n-2} c_1^2 - \dots \mp c_1^n = 0$$
$$d_{n-1} - d_{n-2} c_2 + d_{n-2} c_2^2 - \dots \mp c_2^{n-1} = 0$$
$$e_{n-2} - e_{n-3} c_3 + e_{n-4} c_3^2 - \dots \mp c_3^{n-2} = 0$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$k_2 - k_1 c_{n-1} + c_{n-1}^2 = 0$$
$$l_1 - c_n = 0$$

Alle diese Gleichungen sind für die Koeffizienten $a_1, a_2, \dots a_n$ linear. Wenn man sich also die Grössen $c_1, c_2, \dots c_n$ beliebig gegeben denkt, können daraus die Koeffizienten einer lösbaren Gleichung n-ten Grades bestimmt werden. Wenn man aber, umgekehrt, von den Koeffizienten $a_1, a_2, \dots a_n$ beliebig viele gegeben denkt, bestimmen sich die übrigen, sowie die entsprechende Anzahl der Grössen $c_1, c_2, \dots c_n$ aus den n Bedingungsgleichungen. Da nun die allgemeinen Gleichungen 1-sten, 2-ten, 3-ten und 4-ten Grades lösbar sind; so können in der Gleichung n-ten Grades stets vier, aber niemals mehr als vier (in der verkürzten Gleichung, wo schon $a_1 = 0$ gegeben ist, noch drei, aber nicht mehr) Koeffizienten willkürlich gegeben werden, während die übrigen in bestimmten Beziehungen zu jenen stehen müssen. Diese Beziehungen enthalten, wenn 1, 2, 3 oder 4 der Koeffizienten a gegeben sind, bezw. $n - 1$, $n - 2$, $n - 3$, $n - 4$ Willkürliche und sind darstellbar, wenn das System der n Bedingungsgleichungen für die angenommenen Willkürlichen auflösbar ist, d. h. keine Auflösung einer allgemeinen (lauter willkürliche Koeffizienten besitzenden) Gleichung, welche für irgend eine Potenz irgend einer Unbekannten vom 5-ten oder höheren Grade ist, verlangt.

10) Wenn man in die Ausdrücke, welche die Koeffizienten $a_1, a_2, \dots a_n$ der Gleichung n-ten Grades als symmetrische Funktionen der Wurzeln $x_1, x_2, \dots x_n$ darstellen, für diese Wurzeln die allgemeinen Werthe $x_1 = b_0 + b_1 + b_2 + \dots + b_{n-1}$, $x_2 = b_0 + \alpha b_1 + \alpha^2 b_2 + \dots + \alpha^{n-1} b_{n-1}$ u. s. w. substituirt (vgl. §. 15 der Beiträge zur Theorie der Gleichungen); so erhält man die für die Lösbarkeit erforderlichen n Bedingungsgleichungen durch Vermittlung der Grössen $b_0, b_1, b_2, \dots b_{n-1}$. Da hierin stets $b_0 = -\frac{a_1}{n}$ ist; so hat man es nach Elimination von b_0 nur mit $n - 1$ Unbekannten $b_1, b_2, \dots b_{n-1}$ und ebenso viel Bedingungsgleichungen zu thun. Für die verkürzte Gleichung n-ten Grades, welche wir im Nachstehenden ins Auge fassen, ist $a_1 = 0$, also $b_0 = 0$, und es kommen für diese überhaupt nur $n - 1$ Bedingungsgleichungen in Betracht. Lassen sich dieselben auflösen; so ergeben die daraus hervorgehenden Werthe von $b_1, b_2, \dots b_n$ sofort die n Wurzeln $x_1, x_2, \dots x_n$ der Gleichung n-ten Grades. Diese Auflösung ist natürlich, wenn $n \geq 5$ ist, nur unter Voraussetzung gewisser Beziehungen zwischen den Koeffizienten $a_1, a_2, \dots a_n$ oder zwischen den Grössen $b_1, b_2, \dots b_{n-1}$ möglich. Die Herren E. und U. Dühring haben in dem Buche „Neue Grundmittel und Erfindungen zur Analysis u. s. w." vom Jahre 1884, welches bei der Abfassung des

Manuskriptes meiner Beiträge zur Theorie der Gleichungen noch nicht erschienen war, und welches ich erst nach Veröffentlichung dieser Beiträge kennen gelernt habe, diejenigen Beziehungen zwischen den Grössen a und b, welche auflösbare Gleichungen erzeugen, mittelst eines von ihnen „Werthigkeitsrechnung“ genannten Verfahrens zu ermittlen gesucht. Dieses Verfahren besteht in Folgendem.

Die Substitution der Werthe von $x_1, x_2, \ldots$ in die Ausdrücke für $a_1, a_2, \ldots$ als symmetrische Funktionen der x erzeugt Glieder, deren Koeffizienten Funktionen der Einheitswurzel α und ihrer Potenzen, also Grössen von der Form $F(\alpha)$, bilden. Nach der Dühringschen Darlegung können nun in den Ausdrücken von $a_1, a_2, \ldots$, da diese Grössen als rationale Zahlen einwerthig sind, alle diejenigen Glieder unterdrückt werden, welche mehrwerthig sind, es brauchen also nur die einwerthigen Glieder beibehalten zu werden. Diese einwerthigen Glieder, welche die Summen gleicher Produkte der b bilden, sind diejenigen, deren Koeffizienten $F(\alpha)$ sich auf eine bestimmte ganze Zahl reduziren, durch welche also der Ausdruck für jedes a als eine ganze rationale Funktion der Grössen b erscheint (ohne gerade eine symmetrische Funktion der b zu sein). Diese Glieder nun entsprechen einem Merkmale, das sich so definiren lässt: wenn für n als Primzahl irgend ein Glied des Ausdruckes für $a_1, a_2, \ldots$ mit $F(\alpha) \cdot b_1^{r_1} b_2^{r_2} b_3^{r_3} \ldots$ bezeichnet wird; so sind diejenigen Glieder einwerthig und demnach allein beizubehalten, für welche $r_1 + 2r_2 + 3r_3 + \ldots$ ein Vielfaches von n ist. Hiernach finden Dührings für die verkürzte Gleichung 5-ten Grades $x^5 + a_2 x^3 + a_3 x^2 + a_4 x + a_5 = 0$ auf S. 204 ihres Werkes die 4 Bedingungsgleichungen

$$a_2 = -5(b_1 b_4 + b_2 b_3)$$
$$a_3 = -5(b_1^2 b_3 + b_2^2 b_1 + b_3^2 b_4 + b_4^2 b_2)$$
$$a_4 = -5(b_1^3 b_2 + b_2^3 b_4 + b_3^3 b_1 + b_4^3 b_3 - b_1^2 b_4^2 - b_2^2 b_3^2 + b_1 b_2 b_3 b_4)$$
$$a_5 = -(b_1^5 + b_2^5 + b_3^5 + b_4^5 - 5 b_1^3 b_3 b_4 - 5 b_2^3 b_1 b_3 - 5 b_3^3 b_2 b_4 - 5 b_4^3 b_1 b_2 + 5 b_1^2 b_2^2 b_4 + 5 b_1^2 b_3^2 b_2 + 5 b_2^2 b_4^2 b_3 + 5 b_3^2 b_4^2 b_1)$$

Diese Gleichungen lassen sich nun durch Stiftung spezieller Beziehungen zwischen den Grössen b auflösbar machen: so ergiebt sich für $b_2 = 0$ und $b_3 = 0$

$$a_2 = -5 b_1 b_4 \qquad a_3 = 0 \qquad a_4 = 5 b_1^2 b_4^2 \qquad a_5 = -b_1^5 - b_4^5$$

also $b_1 b_4 = -\frac{a_1}{a_2} = -\frac{a_2}{5}$, mithin $a_4 = \frac{a_2^2}{5}$ und sodann

$$b_1 = \sqrt[5]{-\frac{a_5}{2} \pm \sqrt{\left(\frac{a_2}{5}\right)^5 + \left(\frac{a_5}{2}\right)^2}}$$

$$b_4 = \sqrt[5]{-\frac{a_5}{2} \mp \sqrt{\left(\frac{a_2}{5}\right)^5 + \left(\frac{a_5}{2}\right)^2}}$$

Hiernach würden also $x_1 = b_1 + b_4$, $x_2 = \alpha b_1 + \alpha^4 b_4$, $x_3 = \alpha^2 b_1 + \alpha^3 b_4$, $x_4 = \alpha^3 b_1 + \alpha^2 b_4$, $x_5 = \alpha^4 b_1 + \alpha b_4$ die Wurzeln der Gleichung $x^5 + a_2 x^3 + \frac{a_2^2}{5} x + a_5 = 0$ sein.

11) Ich bestreite nicht die Richtigkeit der mittelst der Dühringschen Werthigkeitsrechnung aufgestellten $n - 1$ Bedingungsgleichungen, bin jedoch der Ansicht, dass diese Rechnung nicht mathematisch begründet ist, jene Formeln also nicht erwiesen und überhaupt zur Auflösung der höheren Gleichungen unzulänglich sind. Zu näherer Bestätigung unterwerfen wir zunächst die nach dem Dühringschen Verfahren gefundene Wurzel einer speziellen Gleichung fünften Grades einer Prüfung.

Nimmt man einmal $a_2 = -5$, $a_4 = \frac{25}{5} = 5$, $a_5 = 2$; so wird $b_1 = \sqrt[5]{-1 + \sqrt{-1 + 1}} = \sqrt[5]{-1}$, $b_4 = \sqrt[5]{-1 - \sqrt{-1+1}} = \sqrt[5]{-1}$, also $x_1 = 2\sqrt[5]{-1}$. Diese Wurzel muss die Gleichung $x^5 - 5x^3 + 5x + 2 = 0$ erfüllen. Eine Substitution dieses Werthes von x_1 für x fordert $-32 - 40(\sqrt[5]{-1})^3 + 10\sqrt[5]{-1} + 2 = 0$, also $\sqrt[5]{-1} - 4(\sqrt[5]{-1})^3 = 3$. Diese Forderung wird zwar durch den reellen Werth von $\sqrt[5]{-1} = -1$ erfüllt: ein komplexer Werth $\sqrt[5]{-1} = e^{\frac{m\pi}{5} i}$ erfüllt sie jedoch nicht, indem z. B. für $\sqrt[5]{-1} = e^{\frac{\pi}{5} i} = \cos 36^0 + \sin 36^0 . i$ $(\sqrt[5]{-1})^3 = \cos 108^0 + \sin 108^0 . i = -\sin 18^0 + \cos 18^0 . i$ die Forderung $3 - \cos 36^0 - 4 \sin 18^0 = (4 \cos 18^0 - \sin 36^0) i$ unmöglich ist.

Für -1 kann man, ohne den algebraischen Werth dieser Grösse zu ändern, jeden in der Form $e^{(2r+1)\pi i}$ enthaltenen Werth setzen: die Grösse $\sqrt[5]{-1} = e^{\frac{2r+1}{5}\pi i}$ hat daher 5 verschiedene Werthe, und diese liefern für die Wurzel $x_1 = b_1 + b_4$ überhaupt 25 verschiedene Werthe, wenn man aber $b_1 = b_4$ hat, 5 verschiedene Werthe $x_1 = 2b_1$. Die erste Frage geht nun dahin, ob jeder dieser Werthe, und wonicht, welcher von ihnen der gegebenen Gleichung fünften Grades entspricht. Der Fundamentalwerth von $\sqrt[5]{-1}$ für $r = 0$ ist $e^{\frac{\pi}{5} i} = \cos 36^0 + \sin 36^0 . i$, und dieser Werth erfüllt die gegebene Gleichung nicht. Auch keiner der 4 Werthe, welche sich für $r = 0, 1, 3, 4$ ergeben, erfüllt dieselbe: nur der für $r = 2$ sich darbietende Werth $e^{\pi i} = -1$, also derjenige Werth, welcher die Substitution von $(-1)^5$ für -1 verlangt, erfüllt die fragliche Gleichung. Die Werthigkeitsrechnung kennzeichnet diesen einzigen zulässigen Werth der Wurzel nicht; sie bedarf also zuvörderst einer Ergänzung, welche darauf zurückzuführen sein wird, dass die Grössen b_1 und b_4 sämmtliche Bedingungsgleichungen erfüllen müssen, eine Bedingung, welche bei der vorstehenden Gleichung durch die Forderung, dass $b_1 b_4$ einen

reellen Werth habe, leicht zu kennzeichnen ist, allgemein aber einer besonderen Feststellung bedarf.

Abgesehen von der vorstehenden Unbestimmtheit, welche durch geeignete Regeln zu beseitigen ist; so erweckt die Begründung der Werthigkeitsrechnung folgende Bedenken.

Die Grösse $\sqrt{c}$ ist zweiwerthig, die Grösse $\sqrt[r]{c}$ ist r-werthig, die n-te Einheitswurzel α ist n-werthig: gleichwohl haben wir uns in einunddemselben Systeme von Schlussfolgerungen unter einer solchen vielwerthigen Grösse doch immer nur einen einzigen ihrer möglichen Werthe vorzustellen. Demzufolge hat man es eigentlich nur mit einwerthigen Grössen, aber mit mehreren Formelsystemen zu thun, in denen die vielwerthigen Grössen verschiedene Werthe, in jedem Systeme jedoch immer einen einzigen bestimmten Werth haben. Wie verträgt sich nun Diess mit der Werthigkeitsrechnung, welche doch den verschiedenen Grössen in derselben Formel mehrfache Werthe zuschreibt?

Diese Frage ist nur zu beantworten, nachdem der wahre Grund der Vielwerthigkeit aufgedeckt ist. Nach der Dühringschen Auffassung (1. u. 2. Kap.) ist eine isolirte negative Grösse $-c$, sowie eine isolirte imaginäre Grösse $\sqrt{-c}$ eine Unmöglichkeit, und zwar soll die Unmöglichkeit in dem Zeichen — oder $\sqrt{-}$, nicht in der dem Zeichen folgenden Grösse c oder $\sqrt{c}$ liegen. Diese für isolirte Grössen bestehende Unmöglichkeit soll nur einen Sinn erhalten, wenn die Grösse mit einer anderen in einen gewissen, durch jenes Zeichen ausgedrückten Operationszusammenhang tritt. Dieser Zusammenhang bedingt alsdann die Vielwerthigkeit oder die Werthigkeit der fraglichen Grösse, insbesondere die Zweiwerthigkeit der Quadratwurzel. Vielwerthigkeit gilt als gleichbedeutend mit Vieldeutigkeit; der letztere Ausdruck wird auf S. 98 sogar für einen Mangel an Erkenntniss erklärt. Ich halte diese Ansichten für grundfalsch und für das Ergebniss der wohl bei den meisten Mathematikern herrschenden Nichterkenntniss des Unterschiedes zwischen Gleichheit und Identität (vgl. §. 13 und 14 der Beiträge zur Theorie der Gleichungen). Solange es sich um Identitäten handelt, kann weder von Vieldeutigkeit, noch von Vielwerthigkeit die Rede sein: die Gleichheit aber, welche nur Übereinstimmung in den Endpunkten verlangt, gestattet die Behaftung der Grösse c mit unendlich verschiedenen Zeichen $(-1)^{2s}$, lässt also diese Grösse als eine vieldeutige erscheinen. Jede Grösse ist daher im Sinne der algebraischen Gleichheit vieldeutig: da jedoch alle diese Werthe sich geometrisch decken; so stellen sie sämmtlich nur einen geometrischen Werth dar, d. h. die vieldeutige Grösse c ist einwerthig. Die r-te Wurzel einer absolut bestimmt gegebenen Grösse c, also $\sqrt[r]{c}$ ist, wie die Grösse c selbst, einwerthig: wird jedoch c als vieldeutige Grösse $(-1)^{2s}c$ aufgefasst; so hat die r-te Wurzel (wenn r eine positive ganze Zahl ist) r verschiedene Werthe, welche durch $\sqrt[r]{c} = (-1)^{\frac{2s}{r}}\sqrt[r]{c} = \alpha^{\frac{sm}{r}}\sqrt[r]{c}$ dargestellt sind: die r-te Wurzel jeder Grösse ist daher r-werthig, überhaupt ist die Wurzelgrösse vielwerthig. Ausserdem aber ist sie, wie jede Grösse, im algebraischen Sinne vieldeutig, indem jeder der r verschiedenen Werthe

noch mit jedem beliebigen Faktor $(-1)^{2t}$ versehen werden kann. Die Vieldeutigkeit der Grössen bedingt daher die Vielwerthigkeit ihrer Wurzeln, und Vieldeutigkeit und Vielwerthigkeit sind zwei ganz verschiedene Begriffe. Die einzelnen Werthe einer vieldeutigen Grösse decken sich geometrisch, die einzelnen Werthe einer vielwerthigen Grösse decken sich geometrisch nicht; den einen wie den andern ist jedoch ein absoluter Zahlwerth gemein, und die Verschiedenheit der Einzelwerthe liegt nur in dem Koeffizienten, welcher als ein Zeichen aufzufassen ist. Für die Einzelwerthe einer vieldeutigen Grösse decken sich diese Zeichen, ohne identisch zu sein: für die Einzelwerthe einer vielwerthigen Grösse decken sich diese Zeichen nicht, sondern stellen verschiedene Richtungskoeffizienten dar. In den Begriffen von Vieldeutigkeit und Vielwerthigkeit haben hiernach die Zeichen durchaus nicht die Bedeutung von Operationszeichen, sondern von Richtungskoeffizienten, sie erscheinen hier als die Symbole, welche die dritte Grundeigenschaft der Grössen, nämlich die Richtung, bezeichnen. Im Ausdrucke $(-1)^{2s} c = (1)^s c = (+) c = + c$ einer positiven Grösse verlangt das Zeichen $+$ durchaus keine Addition, sondern bezeichnet eine Grösse von positiv primärer Richtung; im Ausdrucke $(-1) c = -c$ verlangt das Zeichen $-$ keine Subtraktion, sondern bezeichnet eine Grösse von negativ primärer Richtung; im Ausdrucke $(-1)^{\frac{1}{2}} c = ic$ verlangt das Zeichen i keine Operation, sondern bezeichnet eine Grösse von positiv sekundärer Richtung u. s. w. Dass dieselben Symbole bald als Operationszeichen, bald als Richtungskoeffizienten gebraucht werden, also im ersten Falle eine Operation, wie Addition oder Subtraktion verlangen, im zweiten Falle aber eine Relation oder ein Verhältniss zu der Grundeinheit darstellen, ist eine gewisse Mangelhaftigkeit der mathematischen Symbolik, dient jedoch zur Vereinfachung der Formeln: diese Vielseitigkeit ist nicht allgemein erkannt: die Dühringsche Darstellung trägt jedoch zur Aufklärung Nichts bei, sondern erzeugt eine weitere Verwirrung der Begriffe, indem sie die isolirten negativen und imaginären Grössen für Unmöglichkeiten erklärt, während sie nach Vorstehendem eine leicht verständliche Bedeutung haben.

In §. 14 der Beiträge zur Theorie der Gleichungen habe ich gezeigt, dass auch die Vielheit der Wurzeln einer Gleichung n-ten Grades lediglich aus der Vieldeutigkeit der Koeffizienten $a_1, a_2, \ldots a_n$ entspringt, und dass eine Gleichung mit absolut eindeutigen Koeffizienten nur eine einzige Wurzel haben könnte. Wenn aber die Koeffizienten a vieldeutige Grössen sind; so verliert die Dühringsche Werthigkeitsrechnung ihren Stützpunkt, da die Ausdrücke für diese Koeffizienten unter der ausdrücklichen Voraussetzung entwickelt sind, dass diese Koeffizienten eindeutige Grössen seien, welche nach der Dühringschen Auffassung den einwerthigen gleich zu achten sind. Die Werthigkeitsrechnung ist hiernach nicht prinzipiell begründet, erscheint vielmehr als ein auf ziemlich laxen Grundsätzen erbautes Verfahren.

Was die weitere Ausführung der Dühringschen Werthigkeitsrechnung betrifft; so ist dazu Folgendes zu bemerken. Die Ausdrücke der Koeffizienten $a_2, a_3, \ldots a_n$ in den $n-1$ Bedingungsgleichungen bilden einen Inbegriff von Gliedern. Jedes einzelne derselben besteht aus einem

Faktor $F(\alpha)$, welcher eine Summe von Potenzen der Einheitswurzel α darstellt, und aus einem Faktor $b_1^{r_1}\ b_2^{r_2}\ \ldots$, welcher ein Produkt von Potenzen der Grössen b darstellt (worin einige der Exponenten $r_1, r_2, \ldots$ auch $= 0$ sein können). Ich bezweifle nicht, dass in allen denjenigen Gliedern, in welchen $1 \cdot r_1 + 2 \cdot r_2 + 3 r_3 +$ u. s. w. ein Vielfaches von n ist, der Faktor $F(\alpha)$ eine positive oder negative ganze reelle Zahl ist, und dass sich dieser Faktor in allen übrigen Gliedern vermöge der Beziehung $1 + \alpha + \alpha^2 + \ldots + \alpha^{n-1} = 0$ auf null reduzirt, sodass diese Glieder aus den Bedingungsgleichungen verschwinden. Diese beiden Sätze bedürfen aber eines strengen Beweises, welcher durch den Begriff der Vielwerthigkeit nicht ersetzt werden kann, da dieser Begriff durch die vorstehend bezeichnete Vieldeutigkeit der Koeffizienten a im allgemeinen Gleichungssysteme und durch die Eindeutigkeit dieser Grössen, sowie der Grössen b und der Potenzen von α im besonderen Gleichungssysteme seine Strenge verliert. Sobald aber dieser Beweis erbracht und der spezielle Werth der ganzen reellen Faktoren der übrig bleibenden Glieder nachgewiesen sein wird (was in der nächsten Nummer geschehen soll), tritt die Werthigkeitsrechnung ganz ausser Kraft, sie wird überflüssig.

Ein sehr wesentlicher Einwurf, welchen ich gegen das Dühringsche Verfahren zu machen habe, besteht darin, dass dieses Verfahren, soweit es den Gegenstand des 8. Kapitels ausmacht, nur eine Andeutung über die mögliche Lösung der Aufgabe in den einfachsten Fällen, durchaus keine Vorschrift, nach welcher die Lösung im Allgemeinen geschehen kann, enthält. Indem die Verfasser nämlich in der Form $x = b_1 + b_2 + b_3 + b_4$ der Wurzel der Gleichung 5-ten Grades zwei b, nämlich b_2 und b_3 annulliren, reduziren sie die Aufgabe auf die Bestimmung zweier Unbekannten b_1 und b_4, also auf die Lösung einer quadratischen Gleichung, deren Wurzel entweder die 1-ste, oder die 2-te, oder die 3-te, oder die 4-te, oder die 5-te Potenz des gesuchten b sein kann. Dieser Fall gehört zu den denkbar einfachsten, und es ist ein grosser Irrthum, wenn die Verfasser im 8. Kapitel die Ansicht aussprechen, dass ihr Rechnungsschematismus für die Gleichung 5-ten Grades den Typus für die Behandlung jeder höheren Gleichung abgebe. Das ist durchaus nicht der Fall: denn durch Unterdrückung zweier b bleiben für die Gleichung 6-ten, 7-ten, 8-ten, 9-ten Grades u. s. w. bezw. 3, 4, 5, 6 u. s. w. Unbekannte zu bestimmen, also anstatt der quadratischen Gleichung eine Gleichung 3-ten, 4-ten, 5-ten, 6-ten u. s. w. Grades zu lösen, von welcher irgend eine Potenz eines gesuchten b die Wurzel ist. Eine solche Gleichung mit einer Unbekannten ist aber durch die Dühringschen Bedingungsgleichungen nicht unmittelbar gegeben, sondern muss aus diesen Gleichungen erst durch Elimination der übrigen b abgeleitet werden, wobei es sich ereignen kann, dass die Endgleichung einen sehr hohen Grad annimmt. Die Auflösung derartiger höherer Gleichungen macht aber eben die ganze in Frage stehende Aufgabe aus, diese Aufgabe ist also durch das gedachte Verfahren nicht gelös't, sondern nur verschoben.

Hierzu kömmt, dass die Frage, warum gerade zwei der Grössen b, nicht eine oder deren drei, vier u. s. w. annullirt werden können, bezw.

müssen, keiner Untersuchung unterworfen ist, wodurch die Auflösung eine unvollständige bleibt.

Schliesslich aber ist die Annullirung einzelner Grössen b doch nur ein spezielles Mittel, die Bedingungsgleichungen lösbar zu machen: dieselben können, wie wir in Nr. 15 zeigen werden, auch durch andere Substitutionen lösbar werden: das fragliche Verfahren kann daher keine Allgemeinheit beanspruchen. Allerdings suchen die Verfasser im 9. Kapitel das Lösungsverfahren zu verallgemeinern: allein, nachdem sie auf S. 210 die ungerechtfertigte Behauptung aufgestellt haben, dass die obigen $n-1$ Bedingungsgleichungen zur Herstellung anderer Auflösungen, als solcher, die durch Annullirung gewisser b gewonnen werden, ungeeignet seien (weiter unten in Nr. 15 werden wir die Möglichkeit auch anderer Auflösungen nachweisen), stützen sie im 9. Kapitel auf S. 229 ff. das Lösungsverfahren auf den Satz von Galois, nämlich auf den Satz, dass jede Wurzel einer Gleichung von primem Grade eine rationale Funktion von zwei anderen Wurzeln ist. Dieser Satz gilt nur für Primwerthe von n: ich habe denselben auf S. 57 der Beiträge zur Theorie der Gleichungen in grosser Kürze entwickelt und zugleich auf zusammengesetzte Werthe von n erweitert. Abgesehen nun davon, dass der Galoissche Satz und daher das darauf gestützte Auflösungsverfahren keine Allgemeingültigkeit hat, erscheint dieses Verfahren sehr umständlich und verwickelt und wird durch die Berücksichtigung der zusammengesetzten Werthe von n auf S. 233 ff. des Dühringschen Werkes noch erheblich schwieriger.

12) Im Nachstehenden beabsichtige ich, die Koeffizienten $a_2, a_3, \ldots a_n$, welche Glieder von der Form $F(u) \,.\, b_1^{r_1} b_2^{r_2} \ldots$ bilden, zu entwickeln. Die Exponenten $r_1, r_2, \ldots$ können zum Theil gleich null sein: lässt man jedoch nur Exponenten > 0 zu, was einfacher ist und im Folgenden geschehen soll; so nehmen diese Glieder die Form $F(u) \,.\, b_{s_1}^{r_1} b_{s_2}^{r_2} b_{s_3}^{r_3} \ldots$ an, worin die Zeiger $s_1, s_2, s_3, \ldots$ Werthe > 0 haben. Der Faktor $F(u)$ ergiebt sich (da wir es mit einer verkürzten Gleichung n-ten Grades, worin $a_1 = 0$ ist, zu thun haben) aus der Multiplikation der betreffenden der in §. 15 der Beiträge zur Theorie der Gleichungen aufgestellten Polynome, welche, wenn n eine Primzahl ist, folgende Form haben.

$$
\begin{array}{lll}
x_1 & = & u^0 b_1 + u^0 b_2 + u^0 b_3 + u^0 b_4 + \ldots + u^0 b_{n-1} \\
x_2 & = & u^1 b_1 + u^2 b_2 + u^3 b_3 + u^4 b_4 + \ldots + u^{n-1} b_{n\;1} \\
x_3 & = & u^2 b_1 + u^4 b_2 + u^6 b_3 + u^8 b_4 + \ldots + u^{2n-2} b_{n-1} \\
x_4 & = & u^3 b_1 + u^6 b_2 + u^9 b_3 + u^{12} b_4 + \ldots + u^{3n-3} b_{n-1} \\
x_5 & = & u^4 b_1 + u^8 b_2 + u^{12} b_3 + u^{16} b_4 + \ldots + u^{4n-4} b_{n-1} \\
\cdot & \cdot & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\
x_n & = & u^{n-1} b_1 + u^{2n-2} b_2 + u^{3n-3} b_3 + u^{4n-4} b_4 + \ldots + u^{(n-1)(n-1)} b_{n-1}
\end{array}
$$

Wenn in einem Gliede eine der Grössen b einen Exponenten r hat, welcher > 1 ist; so bedeutet Diess eine r-malige Wiederholung derselben Grösse b: man kann daher alle Glieder aus Grössen b auf erster Potenz mit Wiederholungen zusammengesetzt denken. Betrachten wir zunächst ein solches Glied ohne Wiederholungen, also, wenn wir einmal ein dreidimensionales Glied vor Augen nehmen, ein Glied von der Form

$F(\alpha) \cdot b_s b_t b_u$. Die Aufgabe besteht darin, den zu den gegebenen drei Zeigern s, t, u gehörigen Faktor $F(\alpha)$ zu bestimmen. Die Multiplikation jeder drei beliebigen der vorstehenden n Polynome liefert einen Bestandtheil von $F(\alpha)$, und dieser Bestandtheil stellt das Produkt dreier Potenzen von α oder einer Potenz von α mit einem dreigliedrigen Exponenten dar. Dieser Exponent hat den Werth $cs + dt + eu$, und hierin können die drei Koeffizienten c, d, e alle möglichen Werthe 0, 1, 2, ... $n-1$ mit alleinigem Ausschlusse derjenigen annehmen, in welchen zwei der Grössen c, d, e einander gleich sind (weil Diess der Multiplikation eines Polynoms mit sich selbst entsprechen würde). Es kömmt hiernach wesentlich auf die Ermittelung aller möglichen Kombinationen der drei Koeffizienten c, d, e an, denen wir die Faktoren s, t, u in Gedanken hinzufügen. Wenn c, d, e eine zulässige Kombination ist; so wird auch $c+1$, $d+1$, $e+1$, ferner $c+2$, $d+2$, $e+2$ u. s. w. eine solche sein: man kann also die Kombination c, d, e in vertikaler Richtung der vorstehenden Tafel zyklisch variiren, indem man jedesmal, wo ein solcher Koeffizient $= n$ wird, den Werth 0 dafür setzt. Jede Kombination c, d, e liefert daher eine Gruppe von n Kombinationen, welche beispielsweise für $n = 5$ aus der Kombination 0 1 3 (worunter der Exponent $0s + 1t + 3u$ zu verstehen ist) die Gruppe 0 1 3 1 2 4 2 3 0 3 4 1 4 0 2 erzeugt.

Hiernach handelt es sich um die Bestimmung der verschiedenen möglichen Anfangskombinationen jeder n-gliedrigen Gruppe. Dieselben bilden sich durch die Kombinationen zu drei Elementen aus den n Elementen 0, 1, 2, ... $n-1$, indem man 0 1 2 als die erste Kombination nimmt und nun das letzte Glied fortgesetzt durch Erhöhung um eine Einheit variirt, sobald aber der Werth n erreicht wird, dafür 0 an die Stelle setzt und jede Kombination ausschliesst, in welcher zwei gleiche Zeiger erscheinen. Diese Variation des letzten Gliedes ist so lange fortzusetzen, bis sich die erste Kombination wiederholt: so erhält man z. B. für $n = 5$ die drei Kombinationen 0 1 2 0 1 3 0 1 4, indem die folgende 0 1 0 und die darauf folgende 0 1 1 auszuschliessen sind, die alsdann folgende 0 1 2 aber mit der ersten zusammenfällt. Nach dieser Variation des letzten Gliedes wird das vorletzte um eine Einheit erhöhet und als letztes Glied irgend ein vom ersten und zweiten Gliede verschiedener Werth gesetzt. Diess giebt wiedernm drei Kombinationen 0 2 3 0 2 4 0 2 1. Hierauf folgen nach derselben Regel die drei Kombinationen 0 3 4 0 3 1 0 3 2 und zuletzt die drei Kombinationen 0 4 1 0 4 2 0 4 3. Im Ganzen gehen hieraus für die dreidimensionale Funktion des 5-ten Grades 12 Anfangskombinationen hervor, welche nach dem Vorhergehenden $12 \cdot 5 = 60$ dreigliedrige Exponenten erzeugen. Allgemein erzeugt die m-dimensionale Funktion des n-ten Grades $(n-m+1)(n-m+2) \ldots (n-1) = p$ Anfangskombinationen und eine Gesammtmenge von $pn = (n-m+1)(n-m+2) \ldots n$ m-gliedrigen Exponenten. So würde die vierdimensionale Funktion des 5-ten Grades folgende $2 \cdot 3 \cdot 4 = 24$ Anfangskombinationen

0 1 2 3 0 1 2 4 0 1 3 4 0 1 3 2 0 1 4 2 0 1 4 3 0 2 1 3 0 2 1 4
0 2 3 4 0 2 3 1 0 2 4 1 0 2 4 3 0 3 1 2 0 3 1 4 0 3 2 1 0 3 2 4
0 3 4 1 0 3 4 2 0 4 1 2 0 4 1 3 0 4 2 3 0 4 2 1 0 4 3 1 0 4 3 2

liefern, und eine jede würde eine Gruppe von 5 Kombinationen, z. B. die erste die 5 Kombinationen 0 1 2 3 1 2 3 4 2 3 4 0

3 4 0 1 4 0 1 2, liefern, sodass im Ganzen 120 viergliedrige Exponenten entständen.

Stellt man jetzt die Gesammtheit aller Exponenten in p Reihen, deren jede die n durch zyklische Verschiebung entstehenden Kombinationen, jedoch mit den ursprünglichen, selbst über die Zahl n hinaus gehenden Elementen, enthält, zusammen, indem man die Buchstaben s, t, u ... hinzufügt und jede Kombination, welche einen Exponenten darstellen soll, in Klammern schliesst; so ergiebt sich für das Beispiel $n = 5$, $m = 3$, also $p = 3 . 4 = 12$

$(0s+1t+2u)(1s+2t+3u)(2s+3t+4u)(3s+4t+5u)(4s+5t+6u)$
$(0s+1t+3u)(1s+2t+4u)(2s+3t+5u)(3s+4t+6u)(4s+5t+7u)$
$(0s+1t+4u)(1s+2t+5u)(2s+3t+6u)(3s+4t+7u)(4s+5t+8u)$
$(0s+2t+3u)(1s+3t+4u)(2s+4t+5u)(3s+5t+6u)(4s+6t+7u)$
$(0s+2t+4u)(1s+3t+5u)(2s+4t+6u)(3s+5t+7u)(4s+6t+8u)$
$(0s+2t+6u)(1s+3t+7u)(2s+4t+8u)(3s+5t+9u)(4s+6t+10u)$
$(0s+3t+4u)(1s+4t+5u)(2s+5t+6u)(3s+6t+7u)(4s+7t+8u)$
$(0s+3t+6u)(1s+4t+7u)(2s+5t+8u)(3s+6t+9u)(4s+7t+10u)$
$(0s+3t+7u)(1s+4t+8u)(2s+5t+9u)(3s+6t+10u)(4s+7t+11u)$
$(0s+4t+6u)(1s+5t+7u)(2s+6t+8u)(3s+7t+9u)(4s+8t+10u)$
$(0s+4t+7u)(1s+5t+8u)(2s+6t+9u)(3s+7t+10u)(4s+8t+11u)$
$(0s+4t+8u)(1s+5t+9u)(2s+6t+10u)(3s+7t+11u)(4s+8t+12u)$

Sondert man aus jeder dieser Reihen das erste Glied als gemeinschaftliches Glied ab; so ergiebt sich als zweites Glied für jede Reihe dieselbe Grösse

$0(s+t+u)$, $1(s+t+u)$, $2(s+t+u)$, $3(s+t+u)$, $4(s+t+u)$

welche allgemein aus n Gliedern besteht, deren letztes $(n-1)(s+t+u+\ldots)$ ist. Hiernach ist der Faktor $F(\alpha)$ von $b_s\, b_t\, b_u$ eine Summe von Potenzen von α, welche ein Produkt aus zwei Faktoren bildet: der eine Faktor ist, wenn man $s + t + u + \ldots = c$ setzt,

$$f = \alpha^{0c} + \alpha^{1c} + \alpha^{2c} + \ldots + \alpha^{(n-1)c}$$

und der zweite Faktor ist, wenn man die $m(n-1)$ Anfangsglieder mit $d_1, d_2, \ldots d_{m(n-1)}$ bezeichnet,

$$g = \alpha^{d_1} + \alpha^{d_2} + \ldots + \alpha^{d_{m(n-1)}}$$

sodass man $F(\alpha) = fg$ hat.

Ist die Zeigersumme c kein Vielfaches von n; so ist der Faktor $f = 0$. Es verschwinden also aus dem Ausdrucke jedes Koeffizienten a alle diejenigen Glieder, deren Zeigersumme $c = s + t + u + \ldots$ kein Vielfaches von n ist, weil für diese der Faktor $F(\alpha) = 0$ wird, und es bleiben nur diejenigen Glieder bestehen, deren Zeigersumme c ein Vielfaches von n ist. Für diese Glieder aber ist $f = \alpha^0 + \alpha^n + \alpha^{2n} + \ldots + \alpha^{(n-1)n} = \alpha^0 + \alpha^0 + \ldots + \alpha^0 = n$, folglich $F(\alpha) = ng$, und es kömmt nur noch auf die Bestimmung des Werthes von g an.

Für das dreidimensionale Glied im vorstehenden Beispiele für $n = 5$ ist g die Summe der 12 Potenzen von a, deren Exponenten

$(t + 2u)$, $(t + 3u)$, $(t + 4u)$, $(2t + 3u)$, $(2t + 4u)$, $(2t + u)$, $(3t + 4u)$, $(3t + u)$, $(3t + 2u)$, $(4t + u)$, $(4t + 2u)$, $(4t + 3u)$

sind. Diese Exponenten sind nach dem Model $n = 5$ äquivalent den Exponenten

$(t + 2u)$	$2(t + 2u)$	$3(t + 2u)$	$4(t + 2u)$
$(t + 3u)$	$2(t + 3u)$	$3(t + 3u)$	$4(t + 3u)$
$(t + 4u)$	$2(t + 4u)$	$3(t + 4u)$	$4(t + 4u)$

Setzen wir die Potenzen, welche den ersten 4 Exponenten entsprechen, $= S_{t+2u}$, die Summe der Potenzen der zweiten und dritten Reihe resp. $= S_{t+3u}$ und S_{t+4u}, sodass also $S_{t+2u} = a^{t+2u} + a^{2(t+2u)} + a^{3(t+2u)} + a^{4(t+2u)}$ u. s. w. ist; so ergiebt sich

$$g = S_{t+2u} + S_{t+3u} + S_{t+4u}$$

Jenachdem der Zeiger eines dieser S kongruent 0 oder nicht kongruent 0 nach dem Model $n = 5$ ist; hat dieses S den Werth 4, oder den Werth -1. Beispielsweise ist für

t	u	$t+2u$	$t+3u$	$t+4u$	S_{t+2u}	S_{t+3u}	S_{t+4u}	g
1	2	0	2	4	4	-1	-1	2
2	3	3	1	4	-1	-1	-1	-3

Für ein zweidimensionales Glied $b_s\ b_t$ sind für $n = 5$ die 4 Anfangskombinationen 01 02 03 04, und man hat

$$g = a^t + a^{2t} + a^{3t} + a^{4t} \qquad S_t$$

Hierin kann t einen der Werthe 1, 2, 3, 4 annehmen, es ist also für jeden dieser Werthe $g = -1$.

Für ein vierdimensionales Glied sind für $n = 5$ die $2 \cdot 3 \cdot 4 = 24$ Anfangskombinationen 0123, 0124 u. s. w. schon vorhin angeführt. Man findet danach leicht

$$g = S_{t+2u+3v} + S_{t+2u+4v} + S_{t+3u+2v} + S_{t+3u+4v} + S_{t+4u+2v} + S_{t+4u+3v}$$

Jenachdem der Zeiger eines dieser S kongruent oder inkongruent 0 nach dem Model 5 ist, wird sein Werth $= 4$ oder $= -1$. So erhält man z. B. für $t = 1$, $u = 2$, $v = 3$ $g = -1 - 1 - 1 - 1 + 4 - 1 = -1$.

Ein fünfdimensionales Glied kann für $n = 5$ nur durch Wiederholung einzelner Zeiger, z. B. als $b_s\ b_t\ b_u\ b_v^2$ oder $b_s\ b_t^2\ b_u^2$ oder $b_s\ b_t\ b_u^3$ u. s. w., also in einer der vorläufig zurückgestellten Formen zu Stande kommen.

Allgemein, bestimmt sich für ein m-dimensionales Glied $b_s\ b_t\ b_u\ b_v \ldots$ und für ein beliebiges n der Werth von g aus den Anfangskombinationen $0\ 1\ 2\ 3 \ldots (m-1)$, deren Anzahl nach dem Obigen gleich $(n - m + 1)\ (n - m + 2) \ldots (n - 1)$ ist. Diese Anfangskombinationen zerfallen in $n - 1$ Gruppen von je $(n-m+1)\ (n-m+2) \ldots (n-2) = h$ Kombinationen, wovon die erste Gruppe mit den beiden Ziffern 0 1

beginnt. Bezeichnet man die letzteren, nachdem hinter den Ziffern 0, 1, 2, 3 . . . bezw. die Buchstaben s, t, u, v . . . ergänzt sind, $0\,s = 0$ aber als unwesentlich unterdrückt ist, mit k_1, k_2, . . . k_h; so ist, wenn $\alpha^k + \alpha^{2k} + \alpha^{3k} + \ldots + \alpha^{(n-1)k} = S_k$ gesetzt wird,

$$g = S_{k_1} + S_{k_2} + \ldots + S_{k_h}$$

Es sind jetzt diejenigen Glieder zu betrachten, in welchen unter den Zeigern s, t, u, . . . gleiche Grössen vorkommen. Sind in dem Gliede $b_s\, b_t\, b_u\, b_v \ldots$ zwei Zeiger, z. B. t und u einander gleich, sodass dieses Glied $b_s\, b_t\, b_u\, b_v \ldots = b_s\, b_t^2\, b_v \ldots$ wird; so behalten die Anfangskombinationen die früheren Werthe mit der Einschränkung, dass darin die Koeffizienten von t und u keine Permutation erleiden, indem $dt + eu = et + du = (d+e)t$ ist. Wir drücken Diess dadurch aus, dass wir über die beiden Koeffizienten in den Ausdrücken $c\,d\,e\,\ldots$, welche gleichen Zeigern angehören, einen Bogen ziehen. Die Anzahl der Anfangskombinationen reduzirt sich jetzt auf die Hälfte der vorigen. Beispielsweise hat man für das vierdimensionale Glied $b_s\, b_t^2\, b_v$ für $n = 5$ statt der obigen 24 die nachstehenden 12 Anfangskombinationen

$$0\,\widehat{1\,2}\,3 \quad 0\,\widehat{1\,2}\,4 \quad 0\,\widehat{1\,3}\,4 \quad 0\,\widehat{1\,3}\,2 \quad 0\,\widehat{1\,4}\,2 \quad 0\,\widehat{1\,4}\,3 \quad 0\,\widehat{2\,3}\,4 \quad 0\,\widehat{2\,3}\,1 \quad 0\,\widehat{2\,4}\,1 \quad 0\,\widehat{3\,4}\,1$$
$$0\,\widehat{3\,4}\,2 \quad 0\,\widehat{4\,2}\,3$$

und daher

$$g = S_{t+2t+3v} + S_{t+3t+2v} + S_{t+4t+2v}$$
$$= S_{3t+3v} + S_{4t+2v} + S_{2v}$$

Setzte man $s = t$; so würden die Wiederholungen der gleichen Glieder nicht schon in der Reihe der Anfangsglieder $\widehat{01}\,2\,3$ $\widehat{01}\,2\,4$ u. s. w., sondern in dieser und den späteren Reihen eintreten, indem man z. B. $\widehat{01}\,2\,3 = \widehat{01}\,2\,3$ u. s. w. erhält. Es ist übrigens unnöthig, den ersten Zeiger s einem späteren gleich zu setzen, da man sich unter s, t, u, v . . . jeden beliebigen Zeiger denken kann. Nur wenn alle Zeiger einander gleich werden, kömmt s in der weiter unten zu bezeichnenden Weise mit in Betracht.

Wenn die drei Zeiger t, u, v einander gleich sind, sodass es sich für $n = 5$ um das Glied $b_s\, b_t\, b_t\, b_t = b_s\, b_t^3$ handelt, reduzirt sich die Anzahl der Anfangskombinationen auf die folgenden

$$0\,\widehat{123} \quad 0\,\widehat{124} \quad 0\,\widehat{134} \quad 0\,\widehat{234}$$

und man hat

$$g = S_{t+2t+3t} = S_t$$

Wenn für ein fünfdimensionales Glied $t = u$ und $v = w$ ist, haben die Anfangskombinationen die Form $0\,\widehat{1\,2}\,\widehat{3\,4}$ u. s. w., wenn für ein sechsdimensionales Glied $t = u$, $v = w = x$ ist, haben sie die Form $0\,\widehat{1\,2}\,\widehat{3\,4\,5}$ u. s. w. Immer lassen sich aus den Anfangskombinationen des generellen Falles, wo alle Zeiger verschieden sind, für den speziellen Fall, wo gewisse Zeiger einander gleich sind, leicht diejenigen entnehmen, welche nicht einander gleich, welche also die Anfangskombinationen dieses speziellen Falles sind.

Diese letzteren nun setzen sich im Allgemeinen aus viergliedrigen Gruppen von der Form l, $2l$, $3l$, $4l$ zusammen, welche in dem Ausdrucke für g ein Glied S_l bilden. Das Nämliche gilt auch von jeder aus diesen Anfangskombinationen durch zyklische Variation in vertikaler Richtung erzeugte Gruppe von Kombinationen: allein es sind jetzt zwei besondere Umstände zu berücksichtigen. Zunächst der Umstand, dass sich durch die zyklische Variation Wiederholungen derselben Kombination einstellen, welche auszuschliessen sind. So hat man z. B. für $n = 5$ für das vierdimensionale Glied $t^2 u^2$ die 12 Anfangskombinationen $\widehat{01}\,\widehat{23}$ $\widehat{01}\,\widehat{24}$ $\widehat{01}\,\widehat{34}$ $\widehat{02}\,\widehat{31}$ $\widehat{02}\,\widehat{34}$ $\widehat{02}\,\widehat{41}$ $\widehat{03}\,\widehat{12}$ $\widehat{03}\,\widehat{14}$ $\widehat{03}\,\widehat{24}$ $\widehat{04}\,\widehat{12}$ $\widehat{04}\,\widehat{13}$ $\widehat{44}\,\widehat{23}$, welche vermöge der zyklichen Variation $5 \,.\, 12 = 60$ Kombinationen liefern. Hierin wiederholt sich jedoch jede Kombination einmal: es kommen also nur 30 verschiedene Kombinationen in Betracht.

Der zweite zu berücksichtigende Umstand ist der, dass, wenn die Kombinationen die Form $0\,\widehat{c_1\ c_2 \ldots}\ \widehat{d_1\ d_2 \ldots}\ \widehat{e_1\ e_2 \ldots}$ oder auch $\widehat{c_1\ c_2 \ldots}\ \widehat{d_1\ d_2 \ldots}\ \widehat{e_1\ e_2 \ldots}$ haben, unter der Gesammtheit aller verschiedenen Kombinationen solche vorkommen können, in welchen alle unter den Bogen stehenden Theile Vielfache von n (oder $= 0$) sind, und dass eine jede solche Kombination in dem Werthe von g immer einem Gliede $a^0 = 1$ entspricht. Hiernach ist, wenn h die Anzahl der übrigen viergliedrigen Theile von g bezeichnet,

$$g = q + S_{k_1} + S_{k_2} + \ldots + S_{k_h}$$

Beispielsweise liegt ein Spezialfall dieser Art für $n = 5$ bei dem dreidimensionalen Gliede $b_s\, b_t\, b_t = b_s\, b_t^2$ vor. Die 6 Anfangskombinationen sind dann $0\,\widehat{12}$ $0\,\widehat{13}$ $0\,\widehat{14}$ $0\,\widehat{23}$ $0\,\widehat{24}$ $0\,\widehat{34}$. Die 4 Kombinationen $0\,\widehat{12}$ $0\,\widehat{24}$ $0\,\widehat{31}$ $0\,\widehat{43}$ sind äquivalent (012), 2(012), 3(012), 4(012), geben also das Glied $S_{t+2t} = S_{3t} = -1$. Die 2 Kombinationen $0\,\widehat{14}$ und $0\,\widehat{23}$ liefern aber wegen $1 + 4 = 5$ und $2 + 3 = 5$ zwei Glieder, welche $= 1$ sind; sodass $q = 2$ und $g = 2 - 1 = 1$ ist. Ebenso ergeben für das vierdimensonale Glied $b_t\, b_t\, b_u\, b_u = b_t^2\, b_u^2$ unter den 12 Anfangskombinationen, welche sich wegen der Wiederholungen auf die 6 Kombinationen 0123 0241 0314 0432 0124 0234 reduziren, wenn $t = 1$, $u = 4$ oder $t = 2$, $u = 3$, also überhaupt $t + u = 5$ ist, die ersten vier die Reihe 0123 2(0123), 3(0123) 4(0123), also $S_{t+5u} = S_t$, und zwar wegen der zyklischen vertikalen Variation 5-mal, mithin von $F(a)$ den Theil $5\,S_t$. Die letzten beiden Kombinationen mit ihren zyklischen vertikalen Variationen zerfallen in 0124, 2(0124), 3(0124), 4(0124), ferner in 1230, 2(1230), 3(1230), 4(1230), sowie in die beiden Kombinationen $\widehat{23}\ \widehat{41}$ und $\widehat{41}\ \widehat{32}$, sie liefern also den Theil $S_{t+6u} + S_{3t+3u} + a^0 + a^0 = S_{t+u} + S_{3(t+u)} + 2 = 2\,S_{t+u} + 2$, sodass man $F(a) = 5\,S_t + 2\,S_{t+u} + 2 = 5\,(-1) + 2 \,.\, 4 + 2 = 5$ oder $g = 1$ erhält. Wenn $t + u$ nicht $= 5$ ist, liefern die ersten vier Anfangskombinationen die Funktion S_t nicht 5-mal, sondern nur 4-mal und daneben 4-mal den Werth a^0, sodass alsdann $F(a) = 4\,S_t + 4 + 2\,S_{t+u} + 2 = 4\,S_t + 2\,S_{t+u} + 6 - 4\,(-1) + 2\,(-1) + 6 = 0$ wird.

Sind ausser s alle übrigen $n-1$ Zeiger $t, u, v \ldots$ in dem n-dimensionalen Gliede $b_s\, b_t^{n-1}$ einander gleich; so giebt es nur die eine Anfangskombination $\overbrace{0\,1\,2\ldots(n-1)}$, mithin ist $g = S_{k_1} = S_{(n-1)t} = a^{(n-1)t} + a^{2(n-1)t} + \ldots + a^{(n-1)(n-1)t} = -1$, da t nur einen der Werthe $1, 2, \ldots (n-1)$ haben kann.

Sind sämmtliche Zeiger $s, t, u \ldots$ in dem Gliede b_s^r einander gleich; so giebt es ebenfalls nur eine Anfangskombination $\overbrace{012\ldots(r-1)}$, sodass man $g = S_{r,s} = a^{rs} + a^{2rs} + \ldots + a^{(n-1)rs}$, also $= -1$ oder $= n-1$ hat. Ist aber $r = n$; so hat man für das n-dimensionale Glied b_s^n nicht nur eine einzige Anfangskombination, sondern nur eine einzige Kombination

$$0\,s + 1\,.\,t + 2\,u + \ldots = 0 + 1 + 2 + \ldots + (n-1) = \frac{n(n-1)}{2},$$

weil jetzt eine Permutation in vertikaler Richtung nicht mehr in Betracht kömmt. Ausserdem wird für diesen Fall der Faktor $f = 1$. Die Summe S besteht daher für diesen Fall aus einem einzigen Gliede. Für ein unpaares n ist dieses Glied $g = a^{\frac{n(n-1)}{2}} = a^0 = 1$, also $F(a) = 1$; für ein paares n hat man $g = -1$, also $F(a) = -1$.

Zur Erläuterung wollen wir für $n = 5$ die Werthe der Faktoren $F(a) = fg$ aller nicht verschwindenden Glieder darstellen. Unter den zweidimensionalen Gliedern kommen nur die beiden $b_1\, b_4$ und $b_2\, b_3$ in Betracht, und man hat für jedes derselben nach dem Obigen $g = -1$, also $F(a) = -5$.

Von den dreidimensionalen Gliedern kommen nur die 4 Glieder $b_1\, b_2^2$, $b_2\, b_4^2$, $b_3\, b_1^2$, $b_4\, b_3^2$ in Betracht. Dieselben gehören sämmtlich der Form $b_s\, b_t\, b_t = b_s\, b_t^2$ an, für welche man nach Vorstehendem $g = q + S_{3t} = 2 - 1 = 1$, also $F(a) = 5$ hat.

Von den vierdimensionalen Gliedern kommen $b_1\, b_2\, b_3\, b_4$, $b_1^2\, b_4^2$, $b_2^2\, b_3^2$, $b_1\, b_3^3$, $b_2\, b_1^3$, $b_3\, b_4^3$, $b_4\, b_2^3$ in Betracht. Für das erste Glied ist nach Obigem $g = S_0 + S_4 + S_4 + S_2 + S_2 + S_1 = 4 - 1 - 1 - 1 - 1 - 1 = -1$, also $F(a) = -5$. Für das zweite und dritte Glied ist, wie vorhin gezeigt, $g = 1$, $F(a) = 5$. Für das vierte, fünfte, sechste und siebente Glied ergiebt sich $g = S_{6t} = S_t = -1$, also $F(a) = -5$.

Von den fünfdimensionalen Gliedern kommen die Glieder $b_1\, b_3^2\, b_4^2$, $b_3\, b_1^2\, b_3^2$, $b_1\, b_2^2\, b_4^2$, $b_4\, b_1^2\, b_2^2$, $b_3\, b_4\, b_1^3$, $b_1\, b_3\, b_2^3$, $b_2\, b_4\, b_3^3$, $b_1\, b_2\, b_4^3$, b_1^5, b_2^5, b_3^5, b_4^5 in Betracht. Für das erste, zweite, dritte und vierte Glied ist $q = 2$ und $g = 2 + S_{3t+7u} = 2 + S_{3t+2u} = 2 - 1 = 1$, also $F(a) = 5$. Für das fünfte, sechste, siebente und achte Glied ist $g = S_{t+9u} = S_{t+4u} = S_3 = S_3 = -1$, also $F(a) = -5$. Für das neunte, zehnte, elfte und zwölfte Glied ist nach dem Obigen $g = 1$ und $f = 1$, also $F(a) = 1$.

Hiernach sind die Koeffizienten der verkürzten Gleichung 5-ten Grades

$$\begin{aligned}
a_2 &= -5\, b_1\, b_4 - 5\, b_2\, b_3 \\
-a_3 &= 5\, b_1\, b_2^2 + 5\, b_2\, b_4^2 + 5\, b_3\, b_1^2 + 5\, b_4\, b_3^2 \\
a_4 &= -5b_1b_2b_3b_4 + 5b_1^2b_4^2 + 5b_2^2b_3^2 - 5b_1b_3^3 - 5b_2b_1^3 - 5b_3b_4^3 - 5b_4b_2^3 \\
-a_5 &= 5\, b_1\, b_3^2\, b_4^2 + 5\, b_2\, b_1^2\, b_3^2 + 5\, b_3\, b_2^2\, b_4^2 + 5\, b_4\, b_1^2\, b_2^2 - 5\, b_3\, b_4\, b_1^3 \\
&\quad - 5\, b_1\, b_3\, b_2^3 - 5\, b_2\, b_4\, b_3^3 - 5\, b_1\, b_2\, b_4^3 + b_1^5 + b_2^5 + b_3^5 + b_4^5
\end{aligned}$$

was mit den Dühringschen Angaben übereinstimmt.

Da man für diejenigen Glieder $b_s^{r_1} b_t^{r_2} b_u^{r_3}, \ldots$, in welchen sich Grössen b wiederholen, also unter den Exponenten $r_1, r_2, r_3, \ldots$ Zahlen > 1 vorkommen, genöthigt ist, ausser den Anfangskombinationen die durch zyklische vertikale Variation sich ergebenden, also die Gesammtheit aller Kombinationen vor Augen zu nehmen; so empfiehlt es sich, die Berechnung von $F(\alpha)$ statt auf die $(n-1)$-gliedrigen Ausdrücke von der Form $S_x = \alpha^x + \alpha^{2x} + \alpha^{3x} + \ldots + \alpha^{(n-1)x}$, welche entweder $= n-1$, oder $= -1$ sind, auf die n-gliedrigen Ausdrücke von der Form $T_x = \alpha^{0x} + \alpha^x + \alpha^{2x} + \ldots + \alpha^{(n-1)x} = \alpha_0 + S_x = 1 + S_x$, welche entweder $= n$, oder $= 0$ sind, zu stützen. Alsdann wird die Gesammtheit aller Koeffizienten eines Gliedes $b_s^{r_1} b_t^{r_2} b_u^{r_3} \ldots$ in eine gewisse Anzahl der Grössen T, welche theils $= n$, theils $= 0$ sind, und in eine gewisse Anzahl der Grössen $\alpha^0 = 1$, welche zu jenen T entweder zu addiren, oder davon zu subtrahiren sind, zerfallen. (Die Subtraktion entsteht, wenn man zur Ergänzung gewisser $(n-1)$-gliedrigen S zu n-gliedrigen T genöthigt ist, Anfangsglieder α^0 hinzuzufügen, was eine Neutralisation durch ebenso viel negative α^0 erfordert). Ein T, welches $= n$ ist, besteht aus n Gliedern, welche sämmtlich $= \alpha^0 = 1$ sind, und demzufolge erscheint $F(\alpha)$ als eine Anzahl der Grössen T, welche $= 0$ sind, und einer Anzahl der Grössen α^0, man hat also stets $F(\alpha) = pT + q\alpha^0 = q$, worin q eine positive oder negative ganze Zahl ist, welche, wenn $r_1 s + r_2 t + r_3 u + \ldots$ kein Vielfaches von n ist, den Nullwerth annimmt.

Ausserdem geht man der Berücksichtigung der obigen Spezialitäten aus dem Wege, wenn man für die zu bestimmenden Glieder in die Anfangskombinationen und in die durch zyklische Variation daraus hervorgehenden Kombinationen gleich von vorn herein die Werthe von $s, t, u, \ldots$ einführt, also nicht erst die Kombinationen der Faktoren $c, d, e, \ldots$, sondern sogleich die Kombinationen $cs \,.\, dt \,.\, eu \ldots$ bildet. Die Grössen $cs, dt, eu, \ldots$ stellen die Exponenten der Grösse α in den Werthen der Wurzeln $x_1, x_2, \ldots x_n$ dar, sind also für eine Primzahl n durch folgende Zahlen repräsentirt

für x_1 durch	0	0	0	0	$\ldots$	0
„ x_2 „	1	2	3	4	$\ldots$	$n-1$
„ x_3 „	2	4	6	8	$\ldots$	$2(n-1)$
„ x_4 „	3	6	9	12	$\ldots$	$3(n-1)$
„ x_5 „	4	8	12	16	$\ldots$	$4(n-1)$
. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .
„ x_n „	$(n-1)$	$2(n-1)$	$3(n-1)$	$4(n-1)$	$\ldots$	$(n-1)(n-1)$

Für einen speziellen Werth von n, z. B. für $n = 5$ reduziren sich diese Zahlen

für x_1 auf	0	0	0	0
„ x_2 „	1	2	3	4
„ x_3 „	2	4	1	3
„ x_4 „	3	1	4	2
„ x_5 „	4	3	2	1

aus welchen nun leicht die Werthe von $F(\alpha)$ herzustellen sind.

13) Die vorstehenden Formeln für g setzen eine verkürzte Gleichung n-ten Grades, wofür $a_1 = 0$ ist, voraus. Für die vollständige Gleichung n-ten Grades tritt vor die Reihen von $x_1, x_2, \ldots x_n$ das Glied b_0, für welches man $a_1 = -n b_0$, also $b_0 = -\frac{a_1}{n}$ hat. Die jetzt in Betracht kommenden Glieder haben die Form $F(\alpha) . b_0^r b_s b_t b_u \ldots$ Setzt man $F(\alpha) = f_1 g_1$; so behält f_1 den obigen Werth von f, welcher der Kombination $b_s b_t b_u \ldots$ entspricht. Der Faktor g_1 wird das Produkt des obigen Werthes von g für die Kombination $b_s b_t b_u \ldots$, multiplizirt mit der Grösse $l = p b_0^r$. Bezeichnet man die Dimension von $b_s b_t b_u \ldots$ mit m, also die von $b_0^r b_s b_t b_u \ldots$ mit $m + r$; so stellt p die Anzahl der Kombinationen zu r Elementen aus $n - m$ Elementen dar; es ist also $p = \frac{(n-m)(n-m-1)\ldots(n-m-r+1)}{1 . 2 \ldots r}$. Ist z. B. $n = 5$, $m = 1$, $r = 3$; so ist für das vierdimensionale Glied $b_0^3 b_3$ $p = \frac{4 . 3 . 2}{1 . 2 . 3} = 4$, für $n = 5$, $m = 2$, $r = 2$ ist $p = \frac{3 . 2}{1 . 2} = 3$.

Für den Fall, dass n keine Primzahl ist, lassen sich die Formeln nach §. 15 der Beiträge zur Theorie der Gleichungen leicht erweitern. Man hat dann zu beachten, dass nicht nur $\alpha^0 + \alpha^1 + \ldots + \alpha^{n-1} = 0$ ist, sondern dass dann auch gewisse Theilsummen, z. B. für $n = 4$ die Summe $\alpha^0 + \alpha^2$, für $n = 8$ die Summe $\alpha^0 + \alpha^4$, für $n = 6$ die Summe $\alpha^0 + \alpha^3$, sowie die Summe $\alpha^0 + \alpha^2 + \alpha^4$, für $n = 9$ die Summe $\alpha^0 + \alpha^3 + \alpha^6$ den Nullwerth hat. Der Hauptsatz, dass für alle Kombinationen $b_s^{r_1} b_t^{r_2} b_u^{r_3} \ldots$, für welche $r_1 s + r_2 t + r_3 u + \ldots$ kein Vielfaches von n ist, $F(\alpha) = 0$ wird, während für alle anderen $F(\alpha)$ einen ganzen Zahlwerth annimmt, bleibt auch für ein zusammengesetztes n bestehen.

14) Im Allgemeinen, d. h. abgesehen von gewissen speziellen Fällen, auf welche wir schon in Nr. 4 hingewiesen haben, erfordert die Gleichheit zweier Wurzeln der Gleichung n-ten Grades, dass $b_1 = b_2 = \ldots b_{n-1} = 0$ sei. Daraus folgt, dass alsdann für die verkürzte Gleichung alle Wurzeln $x = 0$ und für die vollständige Gleichung alle Wurzeln $x = b_0$ sein müssen, wodurch sich die letztere Gleichung auf $(x - b_0)^n = x^n - n b_0 x^{n-1} + \frac{n(n-1)}{1 . 2} b_0^2 x^{n-2} - \ldots \mp b_0^n = 0$ reduzirt.

Ebenso muss im Allgemeinen, abgesehen von speziellen Fällen, wenn eine Wurzel $x = b_0 + \alpha^r b_1 + \alpha^{2r} b_2 + \ldots + \alpha^{(n-1)r} b_{n-1}$, worin α die n-te Einheitswurzel darstellt, dem Ausdrucke $c_0 + \beta^s c_1 + \beta^{2s} c_2 + \ldots + \beta^{(m-1)s} c_{m-1}$, worin β die m-te Einheitswurzel bezeichnet, für Primwerthe von n und m gleich sein soll, $b_0 = b_1 = b_2 = \ldots = b_{n-1}$ und $c_0 = c_1 = c_2 = \ldots = c_{n-1}$ sein, wodurch beide Ausdrücke gleich null werden, also die Gleichung $x^n = x^m = 0$ voraussetzen.

Hiernach sind aus jeder generellen Auflösungsrechnung im Allgemeinen, d. h. abgesehen von gewissen Fällen, diejenigen Fälle ausgeschlossen, in welchen die Gleichung gleiche Wurzeln hat, sowie diejenigen, in welchen

sich die Gleichung in mehrere Gleichungen niedrigeren Grades zerlegen lässt. Ob ein Fall dieser Art vorliegt, oder welche Werthe die Koeffizienten $a_1, a_2, \ldots$ annehmen müssen, damit ein solcher Fall zur Erscheinung kömmt, kann nach den früheren Nummern festgestellt werden: man kann aber die generellen Regeln in Anwendung bringen, indem man irgend eine Zerfällung in beliebig viele gleiche oder ungleiche Faktoren 1-sten, 2-ten, 3-ten u. s. w. Grades voraussetzt, die Koeffizienten jedes hierdurch bedingten Faktors nach den generellen Regeln bestimmt, darauf die Multiplikation aller Faktoren vollzieht und die sich daraus für die Gleichung n-ten Grades ergebenden Koeffizienten gleich $a_1, a_2, \ldots$ setzt. Setzt man z. B. die Zerlegung der Gleichung 5-ten Grades $x^5 + a_1 x^4 + \ldots + a_5 = 0$ in eine Gleichung 2-ten und eine Gleichung 3-ten Grades voraus, sodass die linke Seite das Produkt der beiden Faktoren $(x^2 + d_1 x + d_2)(x^3 + e_1 x^2 + e_2 x + e_3) = 0$ darstellt; so bestimmen sich die Koeffizienten d durch die Formeln

$$x_1 = d_0 + d_1$$
$$x_2 = d_0 + \beta d_1$$

worin $\beta = \sqrt{1}$ ist, und die Koeffizienten e durch die Formeln

$$x_3 = e_0 + e_1 + e_2$$
$$x_4 = e_0 + \gamma e_1 + \gamma^2 e_2$$
$$x_5 = e_0 + \gamma^2 e_1 + \gamma e_2$$

worin $\gamma = \sqrt[3]{1}$ ist. Hierauf liefert die Multiplikation der beiden Faktoren die 5 Bedingungsgleichungen

$$a_1 = d_1 + e_1 \qquad a_2 = d_2 + d_1 e_1 + e_2 \qquad a_3 = d_2 e_1 + d_1 e_2 + e_3$$
$$a_4 = d_2 e_2 + d_1 e_3 \qquad a_5 = d_2 e_3$$

15) Das von mir in §. 15 der Beiträge zur Theorie der Gleichungen angegebene allgemeine Merkmal der Lösbarkeit einer Gleichung n-ten Grades, welches fordert, dass alle symmetrischen Grundfunktionen der 1-sten, 2-ten, 3-ten, ... oder n-ten Potenzen der Grössen b symmetrische Funktionen der Wurzeln $x_1, x_2, \ldots x_n$ sein müssen, behält immer Gültigkeit, wobei indess bemerkt sein mag, dass diese symmetrischen Funktionen der x nicht nothwendig ganze rationale Funktionen zu sein brauchen, dass sie vielmehr beliebige symmetrische Funktionen der x oder, was Dasselbe sagt, beliebige Funktionen der Koeffizienten $a_1, a_2, \ldots a_n$ sein müssen. Die letzte Forderung leuchtet ohne Weiteres ein, weil offenbar die Grössen b in einem gesetzlichen Zusammenhange mit den gegebenen Koeffizienten a stehen, also nothwendig Funktionen der a, mithin symmetrische Funktionen der x sein müssen. Die Herstellung solcher Funktionen durch die Annahme geeigneter Beziehungen zwischen den Grössen $x_1, x_2, \ldots x_n$ oder zwischen deren Elementen ist der auf S. 63 der Beiträge zur Theorie der Gleichungen bezeichnete Weg zur Herstellung lösbarer Gleichungen n-ten Grades. Wenn man hierbei darauf ausgeht, geeignete Beziehungen zwischen den Werthen der Wurzeln $x_1, x_2, \ldots$ herzustellen; so zeigen die vorstehenden Nummern 1 bis 9 den einzuschlagenden Weg: wenn man dagegen

beabsichtigt, geeignete Beziehungen zwischen den Elementen der Wurzeln oder zwischen den Grössen b zu ermitteln; so können hierzu die in Nr. 10 bezeichneten n, bezw. $n-1$ Bedingungsgleichungen dienen, welche die Werthe der Koeffizienten a als Funktionen der Wurzeln x oder als Funktionen der Elemente b dieser Wurzeln darstellen.

Das erste dieser beiden Verfahren liefert eine Wurzel x_1 der Gleichung n-ten Grades, abhängig von einer Willkürlichen, und eine reduzirte Gleichung $x^{n-1} + d_1 x^{n-2} + d_2 x^{n-3} + \ldots + d_{n-1} = 0$, deren Wurzeln die übrigen Wurzeln $x_2, x_3, \ldots x_n$ der gegebenen Gleichung sind.

Das zweite Verfahren liefert nicht die Wurzeln x direkt, sondern indirekt vermittelst der Grössen $b_1, b_2, \ldots b_{n-1}$ unabhängig von Willkürlichen. Die reduzirte Gleichung $y^{n-1} + c_1 y^{n-2} + c_2 y^{n-3} + \ldots + c_{n-1} = 0$ ist diejenige, deren Wurzeln die Grössen $b_1, b_2, \ldots b_{n-1}$ sind. Wenn man, wie es in dem Dühringschen Werke geschieht, das ganze System der Bedingungsgleichungen für lösbar und gelös't ansieht, sodass durch die Auflösung derselben alle Grössen b bekannt geworden sind; so hat die reduzirte Gleichung keine Bedeutung mehr, da ihre Auflösung ja nur die schon bekannten Grössen b reproduziren könnte, und wenn sie Diess etwa in besonderen Formen thäte, diese Formen doch nur auf Identitäten beruhen könnten. Beispielsweise ergiebt sich für die in Nr. 10 betrachtete Gleichung 5-ten Grades die reduzirte Gleichung 4-ten Grades, da wegen der Werthe $b_2 = 0$, $b_3 = 0$ die Koeffizienten $c_1 = -(b_1 + b_4)$, $c_2 = b_1 b_4$, $c_3 = 0$, $c_4 = 0$ werden, $y^4 + c_1 y^3 + c_2 y^2 = y^2(y^2 + c_1 y + c_2) = 0$. Dieselbe hat die beiden Wurzeln $y_2 = b_2 = 0$ und $y_3 = b_3 = 0$, ausserdem aber die beiden Wurzeln y_1 und y_4, welche bezw. $= b_1$ und b_4 sind, jetzt aber als die Wurzeln der quadratischen Gleichung $y^2 + c_1 y + c_2 = 0$ in der Form

$$b_1 = -\frac{c_1}{2} + \sqrt{-c_2 + \left(\frac{c_1}{2}\right)^2} \qquad b_4 = -\frac{c_1}{2} - \sqrt{-c_2 + \left(\frac{c_1}{2}\right)^2}$$

erscheinen. Hierin ist $c_1 = -b_1 - b_4$ und $c_2 = b_1 b_4$, folglich

$$b_1 = \frac{b_1 + b_4}{2} \pm \sqrt{-b_1 b_4 + \left(\frac{b_1 + b_4}{2}\right)^2}$$

$$b_4 = \frac{b_1 + b_4}{2} \mp \sqrt{-b_1 b_4 + \left(\frac{b_1 + b_4}{2}\right)^2}$$

Eine Transposition des ersten Gliedes der rechten auf die linke Seite und eine darauf folgende Quadratur lehrt, dass diese Beziehungen zu Identitäten führen.

Die Annahme, dass die n, bezw. $n-1$ Bedingungsgleichungen lösbar und gelös't, also alle b bekannt geworden seien, entzieht der ganzen Operation diejenige Eigenschaft, vermöge welcher sie die Aufstellung eines Lösbarkeitsmerkmals genannt werden kann: denn es wird hierdurch an die Stelle der Auflösung der Gleichung n-ten Grades das Problem der Auflösung von n oder $n-1$ Bedingungsgleichungen, welche selbst Gleichungen vom n-ten Grade enthalten, gesetzt, ohne dass für die Lösbarkeit dieses Systems ein Merkmal angegeben wäre.

Unser, in §. 15 der Beiträge zur Theorie der Gleichungen angegebenes Lösbarkeitsmerkmal ist von dieser Unzulänglichkeit frei: es postulirt einfach, dass die symmetrischen Grundfunktionen der b oder ihrer 1-sten, 2-ten, ... oder n-ten Potenzen symmetrische Funktionen der Wurzeln $x_1, x_2, \ldots$ oder Funktionen der Koeffizienten $a_1, a_2, \ldots$ der gegebenen Gleichung seien. Ob sie Das sind, kann durch die $n-1$ Gleichungen $a_2 = F_2(b)$, $a_3 = F_3(b)$, ... $a_n = F_n(b)$ festgestellt werden, und aus diesen Gleichungen, welche ganze rationale Funktionen der b darstellen und keinen von der Einheitswurzel α abhängigen Faktor enthalten, können die symmetrischen Grundfunktionen entweder der 1-sten, oder der 2-ten, oder der 3-ten, oder, wenn es für keine der niedrigeren Potenzen möglich ist, der n-ten Potenzen, nämlich die Werthe von $b_1^n + b_2^n + \ldots$, $b_1^n b_2^n + b_1^n b_3^n + \ldots$, $b_1^n b_2^n b_3^n + b_1^n b_2^n b_4^n + \ldots$ u. s. w. hergestellt werden, insofern man erforderlichenfalls gewisse b annullirt oder spezielle Werthe dafür einführt. Sind jene symmetrischen Funktionen ohne solche speziellen Werthe gewisser b nicht darstellbar; so ist die gegebene Gleichung unauflösbar und kann nur durch Substitution spezieller Werthe für gewisse b lösbar gemacht werden, indem alsdann gewisse Koeffizienten a dementsprechende spezielle Werthe annehmen. Sind nun für die Potenzen irgend eines Grades r

$$b_1^r + b_2^r + \ldots = -c_1, b_1^r b_2^r + b_1^r b_3^r + \ldots = c_2, b_1^r b_2^r b_3^r + \ldots = -c_3$$

u. s. w.; so hat man, ohne die Grösse $b_1, b_2, \ldots$ selbst zu kennen, die reduzirte Gleichung $(n-1)$-ten Grades

$$y^{n-1} + c_1 y^{n-2} + c_2 y^{n-3} + \ldots + c_{n-1} = 0$$

deren Wurzeln $y_1 = b_1^r$, $y_2 = b_2^r$, $y_3 = b_3^r$ u. s. w. sind. Da die Möglichkeit dieser Gleichung auf speziellen Werthen gewisser b beruhet; so ist in ihr, wenn ein b annullirt worden ist, $c_{n-1} = 0$, wenn zwei b annullirt sind, $c_{n-2} = 0$ und $c_{n-1} = 0$, wenn drei b annullirt sind, $c_{n-3} = 0$, $c_{n-2} = 0$, $c_{n-1} = 0$, überhaupt bedingt die Annullirung von m der Grössen b das Verschwinden der letzten m Glieder der reduzirten Gleichung. Dieselbe wird also

$$y^m (y^{n-m-1} + c_1 y^{n-m-2} + \ldots + c_{n-m-1}) = 0$$

d. h. sie hat m Wurzeln, welche $= 0$ sind, nämlich den m annullirten b entsprechen, und $n-m-1$ Wurzeln, welche die Werthe der r-ten Potenzen der übrigen b darstellen. Die Lösbarkeit der gegebenen Gleichung erfordert nun die Lösbarkeit dieser auf den Grad $n-m-1$ reduzirten Gleichung, und hierfür gelten die den vorstehenden analogen Bedingungen, welche möglicherweise zu weiteren Annullirungen oder Spezialisirungen von Grössen b nöthigen können. Beispielsweise ergeben für $n = 5$ die obigen Ausdrücke für a_2, a_3, a_4, a_5, wenn man $b_2 = 0$ und $b_3 = 0$ setzt, $a_2 = -5 b_1 b_4$, $a_3 = 0$, $a_4 = 5 b_1^2 b_4^2$, $a_5 = -b_1^5 - b_4^5$. Hieraus folgt $-c_1 = b_1^5 + b_4^5 = -a_5$ und $c_2 = b_1^5 b_4^5 = -\left(\frac{a_2}{5}\right)^5$. Die reduzirte Gleichung ist also

$$y^2 \left\{ y^2 + a_5 y - \left(\frac{a_2}{5}\right)^5 \right\} = 0$$

und ergiebt nun ausser den beiden Wurzeln $y_1 = b_2{}^5 = 0$ und $y_2 = b_3{}^5 = 0$ die beiden Wurzeln

$$y_3 = b_1{}^5 = -\frac{a_5}{2} \pm \sqrt{\left(\frac{a_2}{5}\right)^5 + \left(\frac{a_5}{2}\right)^2}$$

$$y_4 = b_4{}^5 = -\frac{a_5}{2} \mp \sqrt{\left(\frac{a_2}{5}\right)^5 + \left(\frac{a_5}{2}\right)^2}$$

also durch Ausziehung der 5-ten Wurzel die Werthe von b_1 und b_4.

Setzt man $b_3 = 0$ und $b_4 = 0$; so erhält man die Bedingungsgleichungen $a_2 = 0$, $a_3 = -5 b_1 b_2{}^2$, $a_4 = -5 b_2 b_1{}^3$, $a_5 = -b_1{}^5 + b_2{}^5$, welche sich in ähnlicher Weise behandeln lassen.

Setzt man die drei Grössen b_2, b_3, b_4 gleich null; so ergiebt sich $a_2 = 0$, $a_3 = 0$, $a_4 = 0$, $a_5 = -b_1{}^5$, was zu der Gleichung $y^1(y + a_5) = 0$ führt, deren Wurzeln $y_1 = b_2{}^5 = 0$, $y_2 = b_3{}^5 = 0$, $y_3 = b_4{}^5 = 0$, $y_4 = b_1{}^5 = -a_5$ sind.

Setzt man alle vier Grössen b_1, b_2, b_3, b_4 gleich null; so werden alle Koeffizienten a gleich null, und man erhält $y^4 = 0$ mit den vier gleichen Wurzeln $y = 0$, denen die verkürzte Gleichung fünften Grades $x^5 = 0$ und die unverkürzte binomische Gleichung $x^5 + d = 0$ entspricht.

Wenn man mehrere der Grössen b einander gleich setzt; so führt diese spezielle Beziehung zu speziellen Gleichungsformen. So ergiebt die Gleichsetzung aller b $a_2 = -10 b^2$, $a_3 = -20 b^3$, $a_4 = -15 b^4$, $a_5 = -4 b^5$. Die symmetrischen Funktionen der b werden hiernach

$$\begin{aligned} -c_1 &= b_1 + b_2 + b_3 + b_4 = 4b \\ c_2 &= b_1 b_2 + b_1 b_3 + b_1 b_4 + b_2 b_3 + b_2 b_4 + b_3 b_4 = 6b^2 \\ -c_3 &= b_1 b_2 b_3 + b_1 b_2 b_4 + b_1 b_3 b_4 + b_2 b_3 b_4 = 4b^3 \\ c_4 &= b_1 b_2 b_3 b_4 = b^4 \end{aligned}$$

und demgemäss hat man

$$y^4 - 4b y^3 + 6b^2 y^2 - 4b^3 y + b^4 = (y - b)^4 = 0$$

Die Gleichung 5-ten Grades, welche diesem Falle entspricht, hat die Wurzeln $x_1 = 4b$, $x_2 = x_3 = x_4 = x_5 = -b$, ist also

$$(x - 4b)(x + b)^4 = x^5 - 10 b^2 x^3 - 20 b^3 x^2 - 15 b^4 x - 4b^5 = 0$$

ganz wie es die Werthe von a_2, a_3, a_4, a_5 verlangen.

Man sieht, es kömmt in allen Fällen behuf Auflösung der gegebenen Gleichung nicht auf die sofortige Ermittlung der Werthe der Grössen b an, womit ja die gegebene Gleichung bereits gelös't, das Auflösungsverfahren also antizipirt oder als schon bekannt vorausgesetzt sein würde: es handelt sich vielmehr zunächst um die Ermittlung der symmetrischen Grundfunktionen der Grössen b oder ihrer Potenzen als Funktionen der Koeffizienten a der gegebenen Gleichung. Da diese Koeffizienten symmetrische Funktionen der Wurzeln x sind; so müssen die symmetrischen Grundfunktionen der Grössen b als symmetrische Funktionen der Wurzeln x erscheinen, und diese Bedingung macht das von mir aufgestellte Lösbarkeitsmerkmal aus, welches, wenn es sich nicht durch beliebige Werthe

der a erfüllt, durch Spezialwerthe der a, welche Spezialwerthe der b bedingen, herbeigeführt werden muss und auf diese Weise die spezielle Form einer lösbaren Gleichung liefert.

Manche dieser speziellen Formen kann nach dem Obigen wohl aus den Bedingungsgleichungen für die Koeffizienten a_1, a_2, a_3 ... durch Substitution spezieller Werthe für gewisse b (wozu auch die Nullwerthe gehören) abgeleitet werden: allgemeiner ist jedoch das in §. 15 der Beiträge zur Theorie der Gleichungen bezeichnete und weiter oben in Nr. 1 an einer Gleichung dritten Grades nochmals erläuterte Verfahren. Dasselbe besteht darin, die Ausdrücke für die symmetrischen Grundfunktionen der $n-1$ Grössen $b_1, b_2, \ldots b_{n-1}$, also die Werthe der Grössen $c_1, c_2, \ldots c_{n-1}$, welche sich aus den allgemeinen Formeln der b als Funktionen der Wurzeln x ergeben, und welche wir die natürlichen Werthe der c nennen wollen, irgend welchen symmetrischen Funktionen der Wurzeln x oder irgend welchen Funktionen der Koeffizienten a gleich zu setzen und die hierdurch gestifteten Gleichungen bei den ferneren Rechnungen als Bedingungen zu berücksichtigen. Hierbei schalte ich die Bemerkung ein, dass sich die Werthe von c nach den auf S. 60 der gedachten Beiträge angegebenen Formeln der b als ganze rationale Funktionen der x ergeben werden, welche von der Einheitswurzel α unabhängig sind, also diese Grösse nicht enthalten können, weil die einer solchen Funktion gleiche Grösse c kein α enthält. Demgemäss sind auch für diejenigen c, welche keine symmetrischen Funktionen der x sind, nur ganze rationale Funktionen der x oder der a einzuführen.

Sodann bemerke ich, dass die natürlichen Werthe der c im Allgemeinen solche Theile enthalten, welche symmetrische Funktionen der x sind, und ausserdem solche Theile, welche keine symmetrischen Funktionen der x sind, dass diese Werthe also, da die ersteren Theile bestimmte Funktionen der a, die letzteren Theile aber durch Substitution der Ausdrücke $x = b_0 + \alpha^r b_1 + \alpha^s b_2 + \ldots$ für die darin enthaltenen x stets als Funktionen der a und b erscheinen, und dass die aus den b bestehenden Theile keine α enthalten können.

Ausserdem hebe ich hervor, dass das System der natürlichen Werthe der $n-1$ Grössen $c_1, c_2, \ldots c_{n-1}$, wenn man darunter die symmetrischen Grundfunktionen der ersten Potenzen der b versteht, denselben gesetzlichen Zusammenhang darstellt, welcher durch das obige System der Werthe der $n-1$ Koeffizienten $a_1, a_2, \ldots a_{n-1}$ als Funktionen der b dargestellt ist (der Koeffizient a_n kömmt in dem ersteren Systeme nicht vor, wohl aber in dem letzteren: in das erstere kann er jedoch durch Substitutionen, welche die Herstellung symmetrischer Funktionen der x bezwecken, eingeführt werden). Die Befriedigung des einen Systems zieht die Befriedigung des anderen nach sich.

Der ganz allgemeine, zur Auflösung der Gleichung n-ten Grades oder zur Herstellung einer lösbaren Gleichung dieses Grades führende Weg besteht nun im Folgendem. Man setzt die symmetrischen Grundfunktionen der Grössen b oder irgend eine ihrer Potenzen bis hinauf zur n-ten irgend welchen beliebigen ganzen rationalen Funktionen der Koeffizienten $a_1, a_2, \ldots a_n$, deren Potenzen bis zum Grade n aufsteigen können (welche also symmetrische Funktionen der x vertreten), gleich. Ist also

$F_1(a)$ eine Funktion von der Form $k_0 + k_1 a_1 + k_2 a_1^2 + \ldots k_1' a_2 + k_2' a_2^2 + \ldots + k_1'' a_3 + k_2'' a_3^2 + \ldots$, worin die Koeffizienten k willkürliche Zahlen bedeuten; so setzt man $c_1 = F_1(a)$, $c_2 = F_2(a), \ldots$ $c_{n-1} = F_{n-1}(a)$.

Die reduzirte Gleichung vom $(n-1)$-ten Grade ist $y^{n-1} + c_1 y^{n-2} + \ldots + c_{n-1} = 0$. Ist dieselbe allgemein, d. h. für beliebige Werthe der c auflösbar; so ergiebt ihre Auflösung in den $n-1$ Werthen der y die Werthe der $n-1$ Grössen $b_1, b_2, \ldots b_{n-1}$ (während stets $b_0 = -\frac{a_1}{n}$ ist), als bestimmte Funktionen der Koeffizienten c. Führt man in diese Funktionen für die c die angenommenen Funktionen $F(a)$ ein; so erscheinen die b als Funktionen der a. Die Koeffizienten a müssen aber auch dem einen oder dem anderen der vorstehend erwähnten Systeme genügen. Wählt man das erste System, welches aus Gleichungen von der Form

$$c = \Phi(b) = G(a, x) = G'(a, b)$$

besteht; so ergiebt eine Substitution der erwähnten Werthe von b, welche nach Maassgabe der willkürlichen Funktionen $F(a)$ Funktionen von a oder von a und $F(a)$ sind, in die Formeln $\Phi(b) = G'(a, b)$ ein System von $n-1$ Gleichungen, in welchen nur die Grössen a vorkommen. Wählt man das zweite System, welches aus Gleichungen von der Form $a = H(b)$ besteht; so liefert diese Substitution ein System von n Gleichungen, in welchen ebenfalls nur die Grössen a vorkommen. Beide Systeme sind gleichwerthig; ein jedes von ihnen bezeichnet die Bedingungen, welche die Koeffizienten a erfüllen müssen, um eine lösbare Gleichung zu liefern. Die Wurzeln dieser Gleichung sind immer in der Form $x = b_0 + \alpha^r b_1 + \alpha^r b_2 + \ldots$ enthalten, worin die b die aus Vorstehendem sich ergebenden Werthe haben. Damit die Koeffizienten a dieser lösbaren Gleichung bestimmt werden können, sind die Funktionen $F(a)$ so einzurichten, dass das letztere System von Bedingungsgleichungen für die Grössen $a_1, a_2, \ldots a_n$ auflösbar wird. Diese Auflösbarkeit des Bedingungssystems kann nun durch eine angemessene Wahl, bezw. Annullirung der Koeffizienten k in der willkürlichen Funktion $F(a)$ stets herbeigeführt werden. Da dieses System, wenn alle c unsymmetrisch sind, doch nur $n-1$, allgemein aber m Gleichungen enthält, wofür $m < n$ ist; so können daraus höchstens m der Grössen a bestimmt werden, es bleiben also höchstens $n-m$ und wenigstens einer der Koeffizienten der Hauptgleichung willkürlich. Wären alle c symmetrisch; so bedürfte es überhaupt keiner Substitutionen, es blieben also dann alle a willkürlich, d. h. die Hauptgleichung wäre allgemein lösbar. Dieser Fall kann jedoch nur eintreten, wenn $n < 5$ ist. Für $n = 5$ sind alle c unsymmetrisch, es erscheinen als unsymmetrische Funktionen der b, in deren Gliedern $b_s^{r_1} b_t^{r_2} b_u^{r_3} \ldots$ die Summe $r_1 s + r_2 t + r_3 u + \ldots$ ein Vielfaches von n, also $\equiv 0 \ mod\ n$ ist. Ebenso erscheinen die Grössen c, welche symmetrische Grundfunktionen der b sind, als unsymmetrische Funktionen der x, in deren Gliedern $x_s^{r_1} x_t^{r_2} x_u^{r_3} \ldots$ die Summen $r_1 s + r_2 t + r_3 u \ldots$ ebenfalls ein bestimmtes Gesetz befolgen. Die letzteren Funktionen der x können aus den ersteren

Funktionen der b sehr leicht abgeleitet werden, wenn man die Grössen a als die Koeffizienten einer vollständigen Gleichung n-ten Grades, also unter Zulassung der Grösse b_0 nach Nr. 13 herstellt. Denn, wenn man beachtet, dass für eine Primzahl n die Wurzel x_{r+1} die allgemeine Form $x_{r+1} = b_0 + \alpha^r b_1 + \alpha^{2r} b_2 + \ldots + \alpha^{(n-1)r} b_{n-1}$ hat, und dass nach §. 15 der Beiträge zur Theorie der Gleichungen die Grösse b_r die allgemeine Form $b_r = x_1 + \alpha^{(n-1)r} x_2 + \alpha^{(n-2)r} x_3 + \ldots + \alpha^r x_n$ oder auch die Form $b_r = x_1 + \alpha^r x_n + \alpha^{2r} x_{n-1} + \ldots + \alpha^{(n-1)r} x_2$ hat; so geht ein x in ein b über, wenn man statt irgend eines b_s die Grösse x_{n+1-s}, also die Zeiger s der Grössen b in die Zeiger $n + 1 - s$ der Grössen x verwandelt (wobei für $s = 0$ statt $n + 1$ der Werth 1 zu nehmen ist). Ist nun in allen Gliedern von a die Summe $r_1 s + r_1 t + r_2 u + \ldots \equiv 0 \ mod\ n$; so hat dieselbe in allen Gliedern, welche Kombinationen der x darstellen, den Werth $r_1 (n + 1 - s) + r_2 (n + 1 - t) + r_3 (n + 1 - u) + \ldots \equiv r_1 + r_2 + r_3 + \ldots \ mod\ n$.

Diese Funktionen der x stellen aber nicht die obigen Grössen c, nämlich nicht die symmetrischen Grundfunktionen der Elemente $b_1, b_2, \ldots b_{n-1}$, sondern die symmetrischen Grundfunktionen der Elemente $b_0, b_1, b_2, \ldots b_{n-1}$ dar. Wenn man die letzteren Grundfunktionen mit C bezeichnet; so enthalten dieselben nur Glieder $x_s^{r_1} x_t^{r_2} x_u^{r_3} \ldots$, worin $r_1 s + r_2 t + r_3 u + \ldots \equiv r_1 + r_2 + r_3 + \ldots \ mod\ n$, oder auch nur solche, worin die Summe $r_1 (s - 1) + r_2 (t - 1) + r_3 (u - 1) + \ldots \equiv 0 \ mod\ n$, also ein Vielfaches von n ist. (So hat man z. B. für $n = 3$ $C_2 = b_0 b_1 + b_0 b_2 + b_1 b_2 = \frac{1}{3} (x_1^2 - x_2 x_3)$ worin im ersten Gliede $r_1 (s - 1) = 2 . 0 = 0$ und im zweiten Gliede $r_1 (s - 1) + r_2 (t - 1) = 1 . 1 + 1 . 2 = 3$ ist). Das System der C besteht aus n, das der c aus $n - 1$ Gleichungen. Aus den Grössen C können die Grössen c nach der Theorie der symmetrischen Funktionen hergestellt werden und liefern alsdann Funktionen von x, deren Zeiger ebenfalls einem bestimmten Gesetze folgen.

Die Grössen c, welche uns hier interessiren, sind, wie schon bemerkt, unsymmetrische Funktionen der x, eine jede von ihnen kann aber in zwei Theile $f(x) + \varphi(x)$ zerlegt werden, wovon der eine Theil $\varphi(x)$ eine symmetrische Funktion der x ist, welche immer durch symmetrische Grundfunktionen der x, mithin als eine Funktion der Koeffizienten a dargestellt werden kann, während der andere Theil $f(x)$ eine unsymmetrische Funktion von x ist; man hat also immer $c = f(x) + f_1(a)$ und es braucht nun für die obige Rechnung nur für den unsymmetrischen Theil $f(x)$ eine symmetrische Funktion der x, also überhaupt eine beliebige Funktion der a substituirt oder $f(x) = F(a)$ gesetzt zu werden. Dass alle Funktionen für c, C, a und ihre Theile, sowie die dafür zu substituirenden Funktionen ganz und rational sind, leuchtet ein.

Alles drehet sich nach dem Obigen jetzt darum, die unsymmetrischen Funktionen c durch die Substitutionen $f(x) = F(a)$ symmetrisch zu machen und die willkürlichen Funktionen $F(a)$ so zu wählen, dass aus diesen Bedingungsgleichungen die Grössen a sich entwickeln lassen. Wird eine Gleichung mit rationalen Koeffizienten vorausgesetzt; so müssen die Funktionen $F(a)$ natürlich von der Beschaffenheit sein, dass sich die

Grössen a in rationaler Form ergeben. Lässt man irrationale Koeffizienten a zu; so ist diese Forderung unnöthig. Wenn man irrationale Koeffizienten a zulassen will, könnte es scheinen, dass jede Rechnung überflüssig wäre, weil man ja alsdann nur für alle b beliebige Werthe anzunehmen braucht, um daraus alle Wurzeln x und auch durch Multiplikation der Faktoren $x - x_1$, $x - x_2$ u. s. w., oder durch die aus Nr. 12 und 13 hervorgehenden Formeln für a alle a zu bestimmen: allein, hierin liegt keine Auflösung unserer Anfgabe, da diese nicht darin besteht, aus lauter gegebenen Wurzeln eine Gleichung zu bilden, sondern die Beziehungen zwischen den Koeffizienten a, von welchen etliche willkürlich bleiben sollen, also die spezielle Form einer lösbaren Gleichung mit ihrem Koeffizientengesetze und ihren Wurzeln zu bestimmen.

Die reduzirte Gleichung vom $(n-1)$-ten Grade ist nur dann allgemein auflösbar, wenn n nicht grösser als 5 ist. Hat n einen höheren Werth; so ist die reduzirte Gleichung $y^{n-1} + c_1 y^{n-2} + \ldots + c_{n-1} = 0$ ganz wie die vorstehende vom Grade n zu behandeln, d. h. indem die Wurzel der reduzirten Gleichung $y = d_0 + \beta^r d_1 + \beta^s d_2 + \ldots$ gesetzt und mit e die symmetrischen Grundfunktionen der Grössen d bezeichnet werden, ist die reduzirte Gleichung vom Grade $n-1$ auf den Grad $n-2$ zu reduziren, was die Gleichung $z^{n-2} + e_1 z^{n-3} + \ldots + e_{n-2} = 0$ ergiebt, deren Wurzeln z die Werthe der Grössen $d_1, d_2, \ldots$ darstellen. Zu diesem Ende sind für die symmetrichen Grundfunktionen e willkürliche Funktionen der Koeffizienten c anzunehmen (wodurch sie symmetrische Funktionen der Wurzeln y oder der Grössen b werden). Hierdurch ergiebt sich ein Bedingungssystem, welches nur die Grössen c enthält, und dessen Auflösung die spezielle Form der auf den $(n-2)$-ten Grad reduzirbaren Gleichung $(n-1)$-ten Grades ergiebt. Eine weitere Substitution in das Bedingungssystem für die Grössen a ergiebt dann die Werthe der Koeffizienten der zweimal reduzirbaren Gleichung n-ten Grades.

Ist n nicht grösser als b; so ist die Gleichung vom $(n-2)$-ten Grade allgemein auflösbar und daher das vorstehende Verfahren ausführbar. Für einen höheren Werth von n ist die zweimal reduzirte Gleichung wiederum auf den Grad $n-3$ zu reduziren. Durch die bei jeder Reduktion einzuführenden willkürlichen Funktionen kann die Auflösbarkeit aller Bedingungssysteme gesichert und demzufolge nach Maassgabe der in §. 15. der Beiträge zur Theorie der Gleichungen aufgestellten generellen Regel die Form der auflösbaren Gleichung jedes Grades nebst der Form jeder reduzirten Gleichung, zugleich aber der Werth der Wurzeln der Hauptgleichung und aller reduzirten Gleichungen bestimmt werden. Die Form der eingeführten willkürlichen Funktionen bedingt die spezielle Formklasse der auflösbaren Gleichungen.

Schliesslich zeige ich noch folgende Druckfehler in den Beiträgen zur Theorie der Gleichungen an.

Seite	18	Zeile	8	von oben	im ersten Gliede	statt	$(-1)^{\frac{2}{3}}$	lies $(-1)^{\frac{1}{3}}$
„	47	„	15	von unten	statt	x_2	lies	a_2
„	62	„	8	von unten	„	a^3	„	a_3
„	63	„	11	von oben	„	$x_1{}^3$	„	$x_1{}^2$

Von dem Verfasser sind folgende Werke erschienen:

Die mechanischen Prinzipien der Ingenieurkunst und Architektur. 2 Bde. Auf Grundlage des englischen Werkes von Moseley.

Die Prinzipien der Hydrostatik und Hydraulik. 2 Bde., enthaltend die Statik und Mechanik der flüssigen und gasförmigen Körper.

Die Theorie der Gewölbe, Futtermauern und eisernen Brücken.

Die Theorie der Festigkeit gegen das Zerknicken.

Die Elastizitätsverhältnisse der Röhren, welche einem hydrostatischen Drucke ausgesetzt sind.

Über Gitter- und Bogenträger.

Über die Festigkeit der Gefässwände, insbesondere über die Haltbarkeit der Dampfkessel.

Imaginäre Arbeit, eine Wirkung der Zentrifugal- und Gyralkraft mit Anwendungen auf die Theorie des Kreisels, des rollenden Rades des Polytropes, des rotirenden Geschosses und des Tischrückens.

Die Ursachen der Dampfkesselexplosionen und das Dampfkesselthermometer als Sicherheitsapparat.

Über das Verhältniss der Arithmetik zur Geometrie, insbesondere über die geometrische Bedeutung der imaginären Zahlen.

Der Situationskalkul, eine arithmetische Darstellung der Geometrie auf Grund abstrakter Auffassung der räumlichen Grössen.

Die unbestimmte Analytik, enthaltend die diophantischen Gleichungen des ersten und zweiten Grades, die endlichen und die periodischen Kettenbrüche, die Theorie der Ungleichheiten, die Kongruenz der Zahlen, die Zahlentheorie u. s. w. in reellen und komplexen Zahlen.

Die Auflösung der algebraischen und transzendenten Gleichungen mit einer und mehreren Unbekannten in reellen und komplexen Zahlen.

Methodus nova aequationem indeterminatam secundi gradus duas incognitas implicantem per numeros integros solvendi. Dissertatio inauguralis.

Die Umbildung der deutschen Rechtschreibung mit Bemerkungen über die Umgestaltung der deutschen **Maassordnungen.**

Körper und Geist. Betrachtungen über den menschlichen Organismus und sein Verhältniss zur Welt.

Die physiologische Optik. Eine Darstellung der Gesetze des Auges. 2 Bde.

Die Gesetze des räumlichen Sehens. Supplement der physiologischen Optik.

Die Theorie der Augenfehler und der Brille.

Sterblichkeit und Versicherungswesen.

Betheiligung am Gewinne und Nationalversorgung.

Die Regelung der Steuer-, Einkommen- und Geldverhältnisse.

Vorschläge für die Alters- und Invalidenversicherung.

Die polydimensionalen Grössen und die vollkommenen Primzahlen.

Die magischen Figuren.

Die Naturgesetze. 4 Theile und 3 Supplemente:

1. Theil die Theorie der Anschauung oder die mathematischen Gesetze.
2. „ „ „ „ Erscheinung „ „ physischen „
3. „ „ „ „ Erkenntniss „ „ logischen „
4. „ „ „ des Bewusstseins „ „ philosophischen „

1. Supplement. Wärme und Elastizität.
2. „ Elektrizität, Galvanismus und Magnetismus.
3. „ Die Theorie des Lichtes.

Die Welt nach menschlicher Auffassung.

Die Grundlagen der Wissenschaft.

Die Hydraulik auf neuen Grundlagen.

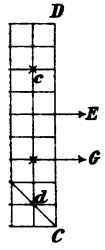
Die Vorbildung für das Staatsbaufach und die Schulreform.

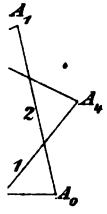
Beiträge zur Theorie der Gleichungen.

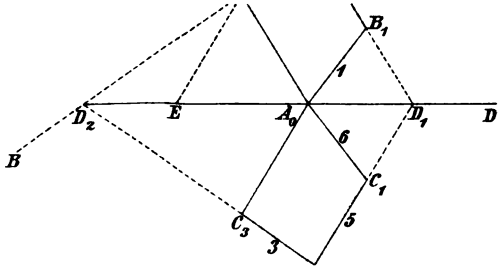
Druck von Friedr. Scheel, Cassel.

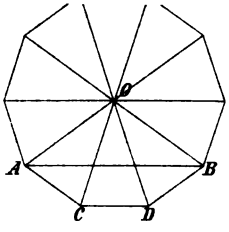
Fig. 6.

Fig. 7.









Von dem Verfasser sind folgende Werke erschienen:

Die mechanischen Prinzipien der Ingenieurkunst und Architektur. 2 Bde.

5. „ Die Theorie des Lichtes.

Die Welt nach menschlicher Auffassung.
Die Grundlagen der Wissenschaft.
Die Hydraulik auf neuen Grundlagen.
Die Vorbildung für das Staatsbaufach und die Schulreform.
Beiträge zur Theorie der Gleichungen.

Druck von Friedr. Scheel, Cassel.

Fig. 6.

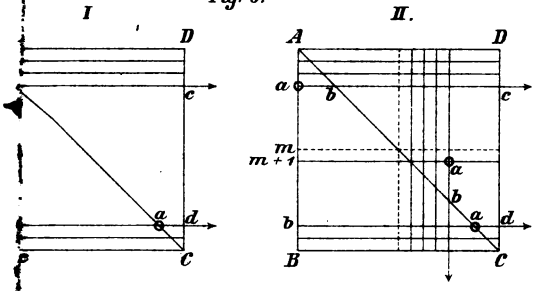


Fig. 7.

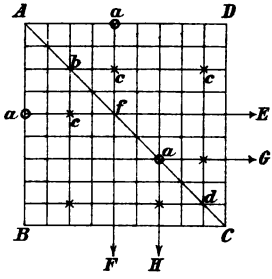


Fig. 8.

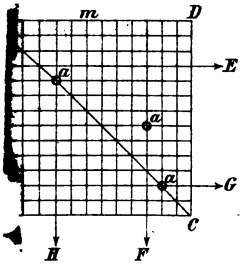


Fig. 9.

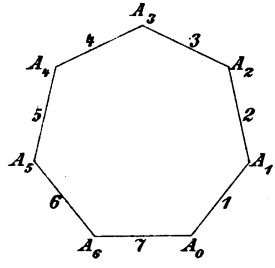


Fig. 10.

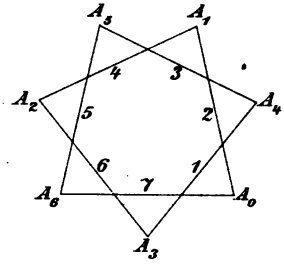


Fig. 11.

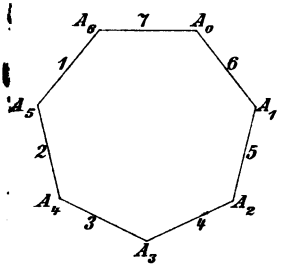


Fig. 12.

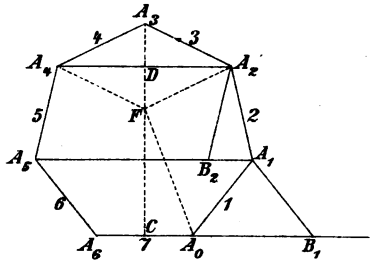


Fig. 13.

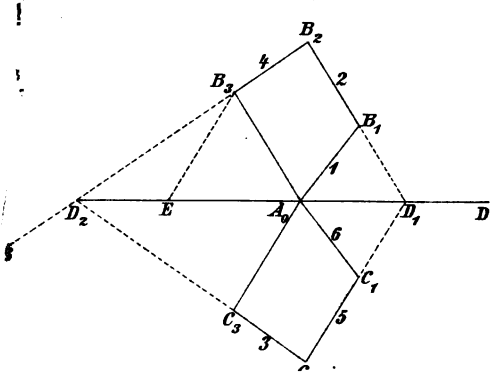
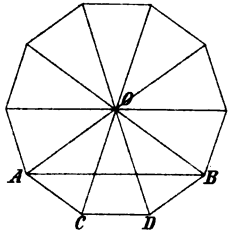



Fig. 14.